

American Medical Association  
Physicians dedicated to the health of America

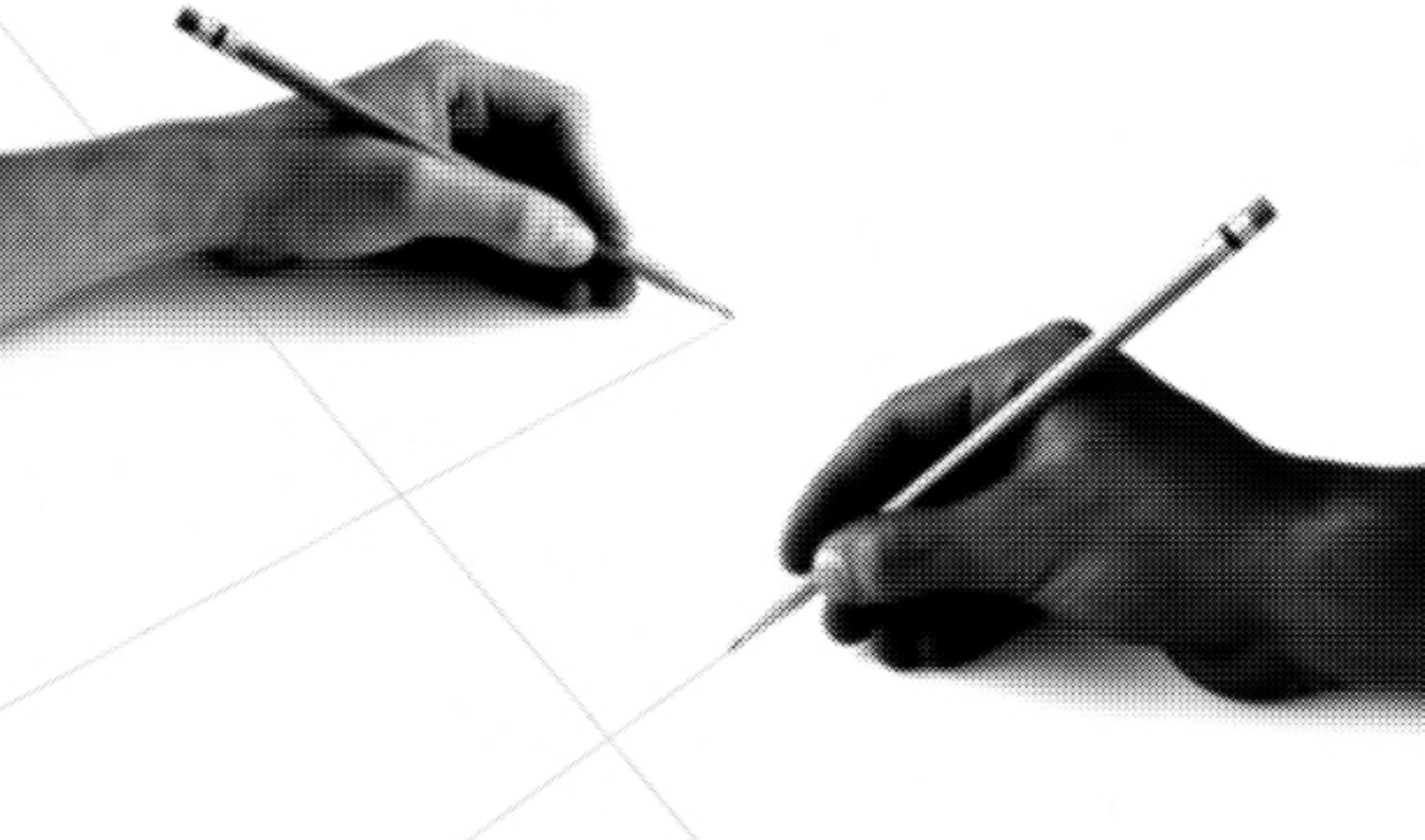


# The **Ethical** Force Program™

**Creating Performance Measures for Ethics in Health Care**

## **The Domain of Health Care Information Privacy**

Protecting Identifiable Health Care Informational Privacy:  
A Consensus Report on Eight Content Areas for Performance  
Measure Development



American Medical Association

Physicians dedicated to the health of America



# The **Ethical** Force Program™

**Creating Performance Measures for Ethics in Health Care**

## **The Domain of Health Care Information Privacy**

Protecting Identifiable Health Care Informational Privacy:  
A Consensus Report on Eight Content Areas for Performance  
Measure Development

### *Disclaimer*

*The views expressed in this report represent a consensus of the Ethical Force Program's Oversight Body members. The report may not reflect the positions of the members' organizations or affiliations. Members of the Ethical Force Program's Expert Advisory Panel on Privacy and Confidentiality served in an advisory capacity to the Oversight Body and neither their own nor their organizations' endorsement of this report should be inferred.*

The Ethical Force Program comes from the Institute for Ethics at the American Medical Association. Permission to produce for non-commercial, educational purposes with display of attribution is granted.

© Ethical Force Program. American Medical Association, December 2000.

ES30:00-447:1M:12/00

# Current Members of the Oversight Body for the Ethical Force Program

(Affiliations listed for identification purposes)

**Myrl Weinberg, CAE (chair)**

National Health Council

**Linda Emanuel, MD, PhD**

Founder

Northwestern University

**Robert Alpert**

UAW Center for Community Health Care Initiatives

**Michele Dennis, RN**

AFSCME

**John Eisenberg, MD**

Agency for Health Care Research and Quality

**Ezekiel Emanuel, MD, PhD**

Warren Magnuson Clinical Center National Institutes of Health

**Mary Jane England, MD**

Washington Business Group on Health

**Arnold Epstein, MD**

Harvard School of Public Health

**David Fleming, MD**

Woodland Clinic

**Larry Gage**

National Association of Public Hospitals and Health Systems

**George Isham, MD**

HealthPartners

**Allan Korn, MD**

National Blue Cross Blue Shield Association

**Catherine Kunkle**

National Business Coalition on Health

**John Ludden, MD**

Tufts University Medical School

**Gladys White, PhD, RN**

American Nurses Association

**John Combes, MD**

American Hospital Association

**Thomas Reardon, MD**

American Medical Association

**Frank Riddick, MD**

Alton Ochsner Medical Foundation

**James Sabin, MD**

Harvard Medical School and Harvard-Pilgrim HealthCare

**Neil Schlackman, MD**

Aetna U.S Healthcare

**Paul Schyve, MD**

Joint Commission on Accreditation of Healthcare Organizations

**Linda Shelton**

National Committee for Quality Assurance

**Drew Smith, JD**

American Association of Retired Persons

**Program Staff**

**Matthew Wynia, MD, MPH**

Executive Director

**Deborah Cummins, PhD**

Associate Director

# Table of Contents

Executive Summary ..... 3  
Summary Figure ..... 5  
Preface ..... 6  
Introduction..... 7  
Background..... 8  
Existing Community Norms/Standards..... 10  
E-Force: Measuring the Quality of Privacy and Confidentiality Protections ..... 12  
Reading Notes..... 13

## ***Content Areas and Associated Measurable Expectations for the Protection of Privacy in Health Care***

Area 1. *Transparency*..... 14  
Area 2. *Consent*..... 15  
Area 3. *Collection Limitation* ..... 17  
Area 4. *Security* ..... 18  
Area 5. *Individual Access* ..... 19  
Area 6. *Data Quality* ..... 20  
Area 7. *Information Use Limitations* ..... 20  
Area 8. *Accountability* ..... 21  
Glossary..... 23

### ***Appendix 1:***

*Some Notes on the “Data Disclosure Board”* ..... 24

### ***Appendix 2:***

*Members of the Ethical Force Oversight Body and of the Expert Advisory Panel on Privacy and Confidentiality*..... 26

**References** ..... 28

# Executive Summary

The Ethical Force Program (E-Force) is a collaborative process to create performance measures for domains of ethics that will be applicable for all participants in health care delivery.

The E-Force program is based on the understanding that all participants in the health care delivery system share certain core ethical obligations by virtue of their participation in this unique enterprise. This document reflects this belief that, although ethical standards may legitimately vary across business, public health, personal, and professional relations, in health care a core set of ethical expectations is critical and must be shared. Furthermore, valid, reliable, and feasible measures of performance on these core expectations would be meaningful and useful for health care decision making.

One of the first ethical domains that the E-Force program is investigating for performance measure development is the protection of identifiable health information throughout the health care system. As one step in a rigorous performance measures development process, the E-Force Oversight Body—consisting of leaders from business, unions, health care delivery organizations, professional and patient organizations, government, and accrediting bodies, and with additional input from an Expert Advisory Panel on Privacy and Confidentiality—has reached consensus on a framework for assessing the adequacy of health information privacy protections throughout the health care system.

In this report, protections to safeguard privacy and confidentiality are defined in eight “content areas.” Each content area then has a set of specific “measurable expectations” on which performance could be measured. In the next phase of this project, the Ethical Force Program will develop performance measures based on these expectations. Readers’ comments will inform the creation and testing of these performance measures.

The eight content areas are as follows:

**Area 1. Transparency**—Health information trustees should make publicly available clear explanations of their policies, procedures, and practices regarding the collection, storage, and use of personally identifiable health information.

**Area 2. Consent**—Whenever feasible, health information trustees should obtain valid informed consent from individuals for the collection, storage, or use of personally identifiable health information. If consent is not obtained, then a formal, authoritative, and publicly accountable process must be used to authorize a waiver of consent.

**Area 3. Collection Limitation**—Health information trustees should limit collection of health information to that information required for current needs, or reasonably projected future needs, which are made explicit at the time consent is obtained.

**Area 4. Security**—Health information trustees should protect the identifiable health information in their care by means of reasonable security measures appropriate to the sensitivity of the information. A specific individual or group should be identified as being responsible for overall security mechanisms and processes.

**Area 5. Individual Access**—Individuals should be allowed access to view and amend or append information to their personally identifiable health information records.

**Area 6. Data Quality**—Health information trustees should seek to ensure that the identifiable health information in their care is as accurate, complete, and up-to-date as is required for the purposes for which it is collected and used.

**Area 7. Information Use Limitation**—Health information trustees should limit the disclosure and use of personally identifiable health information to those purposes that are made explicit at the time consent is obtained or are otherwise authorized through a formal, authoritative, and publicly accountable mechanism.

**Area 8. Accountability**—Health information trustees should be accountable for adhering to standards for the collection, storage, and use of personally identifiable health information, including the responsible transfer of information to other accountable information trustees.

In detailing the expectations that arise within each of these content areas, the report includes several main points of interest.

**Health Information Trustees:** Every individual or organization that creates, accesses, stores, transmits, or uses personally identifiable health information has that information as a result of patient trust. Thus, every such individual or organization is a health information trustee and should understand and accept the responsibilities that come with this entrusted and privileged position. With few exceptions, which are specifically noted, the ethical expectations laid out in this document apply to every health information trustee.

**De-identification:** This report considers only the protection of personally identifiable health information. Information that has been de-identified is not covered. Thus, for example, the use of de-identified billing data sets for health services research is not covered. However, this brings up a complex question: how de-identified is de-identified enough? Every individual or organization entrusted with health information should explicitly define

what level of de-identification is sufficient for specified purposes, and decisions of health information trustees in this regard should be made publicly available.

**Legal Requirements:** Health information trustees should obey the law in regard to privacy and confidentiality. In addition, any individual or organization accessing identifiable health information, including law enforcement agencies, public health agencies, and others with legal authorization to access identifiable data, should live up to fundamental ethical expectations regarding the appropriate protections for and uses of this information (that is, all are health information trustees). As with other personal property, such as one's car, home, or bank records, a court order should usually be required for a legal authority to search an individual's identifiable health information. When identifiable health information is released without consent to a legal authority, it should be delivered with a cover letter to remind the recipient of the sensitive nature of the information being entrusted to him or her.

**Informed Consent:** This report considers primarily those uses of information for which informed consent is not obtained. Under well-accepted principles of autonomy and respect for persons, virtually any use of health information is acceptable if valid informed consent is obtained. Valid informed consent for the collection, storage, and use of identifiable health information would entail disclosure of all necessary information that a reasonable person would use in making an informed decision, in a format that is readily understandable to the individual, and without coercion influencing choice.

**Direct Therapeutic Benefit:** Except for one issue (private, out-of-pocket payment for care), this document deals with uses of identifiable health information that do not confer direct therapeutic or diagnostic benefit on the person whose information is at issue. When information is shared between health care practitioners for the direct therapeutic benefit of the patient, no additional informed consent process is generally required, though it is sometimes desirable that patients be allowed to decline the release of some information even for such purposes. In this report, the use of information for payment of claims is also considered to confer direct benefit to patients. However, if a patient pays out-of-pocket for a service, without requesting insurance reimbursement, then the patient should be allowed to decline any further circulation of information arising from this service, except as required by law.

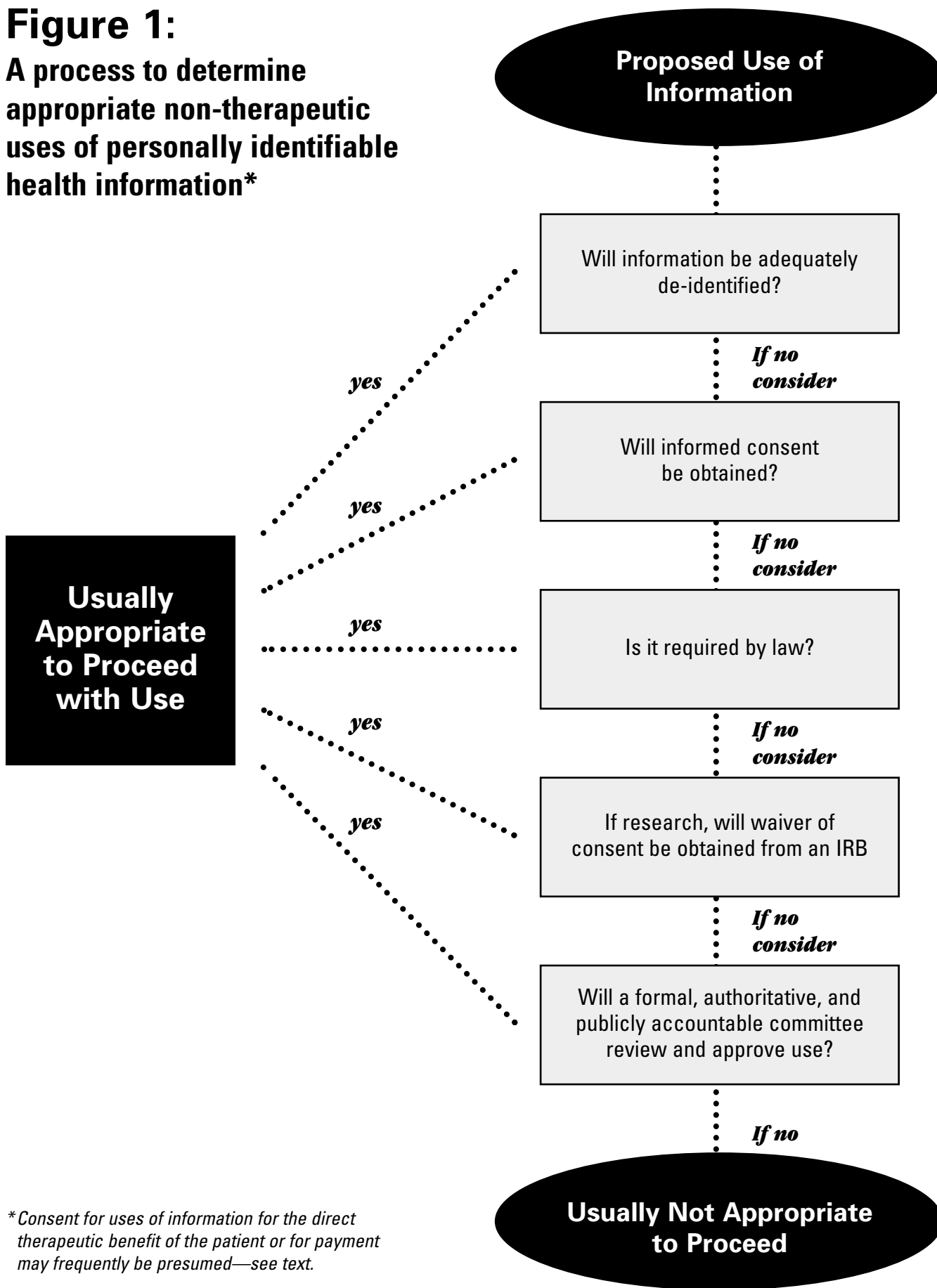
**Publicly Accountable Review Process:** Every use of identifiable health information without consent should receive publicly accountable review and oversight. It is not possible, or feasible, to obtain valid informed consent for every legitimate use of identifiable health information, yet every use of identifiable health information requires some form of accountable review to ensure its legitimacy.

Therefore, formal, authoritative, and publicly accountable processes should be established through which waivers of informed consent might be granted. Certain uses of health information already undergo scrutiny by formal, accountable mechanisms, such as institutional review boards (IRBs) in the case of some medical research. These do not require additional review. For many other uses of identifiable health information without informed consent there currently is little or no formal oversight or meaningful public accountability. A formal, authoritative, and publicly accountable process should exist to review every instance in which personally identifiable health information is used without valid informed consent. One such process, a data disclosure board, is described in more detail.

**Review Process Specifications:** A formal, authoritative, and publicly accountable process that can grant waivers of informed consent should include public/patient advocates in the process as well as clinicians and others. The rationales it has used to justify specific waivers should be publicly available. There should be written records for each proposed use of identifiable health information reviewed. It should grant waivers of consent for categories of uses of information when this is appropriate (such as the use of identifiable patient information for a regular peer review activity) and review such "routine" uses periodically. Some national or regional standards could also be established for some routine uses of identifiable health information.

Figure 1 illustrates a staged process for evaluating the appropriateness of any new proposed use of personally identifiable health information, showing several potential levels of legitimate authorization. Appendix 1 contains descriptive information regarding an example of a formal, authoritative, and publicly accountable mechanism to review proposed waivers of informed consent (a data disclosure board).

**Figure 1:**  
**A process to determine appropriate non-therapeutic uses of personally identifiable health information\***



\*Consent for uses of information for the direct therapeutic benefit of the patient or for payment may frequently be presumed—see text.

## Preface

**Background on the Ethical Force Program and the Expert Advisory Panel.** Today, every participant in health care delivery can be strongly affected by the ethical standards of many other participants. In contemporary health care, there are business, public health, personal, and medical professional ethical standards at work; and all, from time to time, may conflict. The balancing of these various standards necessitates the creation of a “mutual and multilateral web of accountability for ethics” among all participants in health care.<sup>1</sup> Yet, for such accountability to succeed, we will need valid, reliable, and feasible performance measures for each domain of ethics.<sup>2</sup> *The Ethical Force Program (E-Force) mission is to improve health care by fostering the ethical behavior of all participants.* Through the collaborative involvement of major participants in health care, E-Force aims to achieve three goals: (1) to identify and promote ethical expectations for all participants in health care, (2) to develop valid and reliable measures of achievement of ethical expectations, and (3) to encourage the widespread adoption and use of these expectations and measures. To ensure the content validity of the performance measures it creates, the program is being developed in a consensus process, with collaboration among numerous participants in the health care delivery system (individuals involved in this process are listed in Appendix 2).

One important domain of health care ethics that has been selected by the E-Force Program for performance measure development is the protection of health care informational privacy. The accurate and timely collection, storage, and use of individuals' health information is necessary for effective health care delivery and the protection of public health and safety,<sup>3,6</sup> yet justifiable concerns are prevalent regarding the confidentiality of personal health information.<sup>7-11</sup> These concerns have led the National Committee on Vital and Health Statistics to declare that “the United States is in the midst of a health privacy crisis.”<sup>8</sup> The E-Force Program believes that one way out of this crisis lies in developing acceptable expectations for the protection of health information privacy for all participants in health care delivery, and then being able to measure when these expectations are being met. Therefore, this document will form the basis for a set of testable performance measures, which can be validated and then used to assess how well various parties to health care delivery protect the privacy interests of patients and the confidentiality of the identifiable health information entrusted to them.

Given that there are numerous important values at stake in health care,<sup>4, 12, 13</sup> it is important to note at the outset that this document looks primarily to the protection of privacy and

confidentiality and only indirectly at other important values. The Ethical Force Program aims to create similar documents and corresponding sets of measures for many other important domains of health care ethics.<sup>2</sup> Eventually, use of the full spectrum of E-Force Performance Measures for Ethics will allow participants in health care delivery to study the quality of their own and others' overall ethics-related policies, practices, and performance. The measures suggested by this document represent only the first step in this development process.

**Consensus Process Methods.** Performance measures for ethics in the domain of health care informational privacy were created and validated by means of a stepwise approach. The E-Force Oversight Body, in the summer of 1998, appointed a national Expert Advisory Panel (EAP) on Privacy and Confidentiality, consisting of experts in medicine, privacy, ethics, law, accreditation, informatics, and public health (members of the EAP are listed in Appendix 2). The charge of the EAP was to examine existing norms for privacy protections and to suggest shared expectations for performance on protecting the privacy and confidentiality of health information. The EAP reviewed the literature and existing policies—using three meetings, several conference calls, and electronic mail to facilitate communication among EAP members between September 1998 and June 1999.

In June 1999, the EAP reported to the Oversight Body that the ethical domain of health care informational privacy could be broken down into eight content areas, and it suggested a large number of potentially measurable expectations to consider within each content area.

**Role of the Oversight Body.** The Oversight Body—which includes leaders and experts in policy, ethics, accreditation, medicine, managed care, and patient representatives (Appendix 2)—reviewed and suggested revisions to the content areas and expectations. A revised set of measurable expectations was then circulated to the EAP and the Oversight Body. Each member graded each expectation from 1 to 10 in three areas, addressing the importance and universal applicability of the expectation and the feasibility of meeting the expectation. Those that fell below a mean score of 7.5 on any single rating scale were reconsidered by the EAP, and many were eliminated. This newly revised set of expectations was then sent to Oversight Body members for another set of grades on whether each was (1) important, (2) universally applicable, (3) feasible to measure, and (4) realistic to implement. Oversight Body members were free to engage colleagues at their home institutions when assigning grades. Those that did not rate a mean score greater than 7 on all four scales were reconsidered at an Oversight Body meeting in January 2000, and several were combined, revised, or eliminated. In the end, expectations were retained only if the entire Oversight Body

agreed that they should be used as potential subjects of performance measurement. Some were retained with recognition that they might be difficult to measure, because the only way to assess whether such difficulties will arise is to develop measures based on these expectations and then field-test the measures.

In the second stage of this project, these measurable expectations will be used to develop actual performance measures for privacy and confidentiality: survey items; site review, policy review, and document review criteria; and outcomes testing criteria, all of which will be validated before being released for possible implementation.

When taken together, the eight content areas described herein constitute a fairly robust picture of possible areas for privacy and confidentiality protections—though they are by no means exhaustive. The content areas were derived from numerous other sources and rest on broadly accepted community norms for fair information practices (see Introduction below).

As each content area is introduced, it is described and delineated in terms of its ethical and practical justifications and implications. Each such description and explanation is followed by a list of measurable expectations for a party's attention to the content area, from which actual performance measures will be created for testing and validation.

The following Introduction provides some definitions and historical background. We hope that these introductory materials will be useful, but we have also provided a second, more abbreviated, set of "reading notes" on page 13, just before the main body of the report. The reading notes contain information necessary to understand the formatting and interpretation of the subsequent content areas and associated expectations. For those with more limited time, it will be worthwhile to read these comments before moving to the main body of the report.

## Introduction

Those involved in health care information management frequently think of health care information as following a path from (a) data collection, to (b) data storage, then to (c) data accessing and use. When privacy interests are considered, each step on this path deserves its own sorts of protections. Meanwhile, others involved in the health information privacy debates have focused more on asserting a fundamental human "right to privacy."<sup>9, 14-18</sup> Still others have focused on a set of principles termed "fair information practices."<sup>19, 20</sup> These various conceptualizations, concerns, and principles, as one might expect, have tremendous areas of overlap. Wherever possible, we have emphasized these areas of overlap, and we have considered all of these points of view in producing this document.

**Definitions.** Throughout this document we use terminology that has not always had clear and uniform meaning, yet we intend to use terms precisely. Thus, this section sets out core concepts and describes the context in which the subsequent content areas and measurable elements should be viewed. A glossary at the end of the document provides definitions for some additional terms used in the text.

A first step in our work was to differentiate between three distinct but related concepts: privacy, confidentiality, and security. In the United States, the public tends to group many kinds of privacy interests together, from informational privacy to reproductive choice and from sexual activity and orientation to freedom from surveillance.<sup>4</sup> Indeed, the very notion of privacy means so much to so many that some have argued it should be abandoned as meaningless and confusing. However, *privacy has a long and important conceptual and legal history*, and many are reluctant to give up on attempts to define and use some meaningful notion of a "right," or at least an "interest," in privacy. Moreover, even without broad social agreement on what is entailed by a right to privacy, it is useful for the purposes of this document to define what we mean when we use the following terms relating to privacy.

We take *privacy* to be the interest individuals have in their personal control over sensitive aspects of their lives. Any number of aspects of a person's life may be sensitive, but information about oneself is a frequent privacy concern; this is called informational privacy. It is informational privacy with which we are specifically concerned in this document. *Informational privacy* encompasses an individual's interest in whether or not to disclose personal information to others and for what purpose(s).<sup>14, 15</sup> We agree that informational privacy may be described as concerning an

“individual's freedom from excessive intrusion in the quest for information and an individual's ability to choose the extent and circumstances under which his or her beliefs, behaviors, opinions, and attitudes will be shared with or withheld from others.”<sup>21</sup> Health informational privacy is this interest as it pertains to information about one's health status or history.

*Confidentiality* is a promise of limitations on the use and disclosure of information that has been entrusted to one party by another. Confidentiality protections consist of policies and procedures that provide assurances about the promised limitations.<sup>15</sup> The recipient of identifiable health information holds it in trust so that, although this given information is no longer strictly private, it requires a high degree of protection to prevent its further dissemination or use against the wishes of the information source.

Note that a promise of confidentiality is what allows one party to feel that it is safe to give sensitive information to another. And to be effective, such a promise must be reliable. As the National Research Council has written, confidentiality “refers broadly to a quality or condition accorded to information as an obligation not to transmit that information to an unauthorized party...[But] confidentiality has meaning only when the promises made to a data provider can be delivered, that is, the data gatherer must have the will, technical ability, and moral and legal authority to protect the data.”<sup>21</sup>

*Security* encompasses the set of technical and administrative procedures and policies that protect sensitive information from loss or unauthorized disclosure, access, destruction, alteration, or use. Security measures are applied to the people, information, and technologies that collect, store, and use information. Security measures are utilized because of the need to ensure that the confidentiality promise regarding entrusted information is upheld.

## Background

### ***Improved Information Exchange: Benefits and Risks.***

Improved access to relevant health care information can lead to increased efficiency, improved patient outcomes, and lower costs throughout the health care system. Indeed, such improvements as a result of advances in information networks have been documented in several recent studies.<sup>5, 22</sup> Moreover, technological innovations in *computerized health records offer some opportunities for improved security compared to paper records*,<sup>23-25</sup> which all too frequently lie unprotected along hospital corridors, in nursing stations, and at patient bedsides.<sup>26</sup> Yet the public and lawmakers are worried about inconsistent health care information privacy standards; and public concerns about the privacy and confidentiality of health care information appear to encompass more than fear over losing insurance, or a job, if sensitive information is used inappropriately. Opinion polls demonstrate public concern about a fundamental loss of control over the sharing and use of personal health care information. For example, in a 1993 survey, 64% of those surveyed stated that their permission should be asked before their records could be used in medical research even if names were removed from the records.<sup>27</sup> Moreover, a majority of the public, including more than half of nurses and physicians, said that using computers in medical practice would allow access to records by unauthorized people and weaken confidentiality. Recent surveys show no decline in these concerns.<sup>28</sup>

While some worry about inadequate privacy protections, others, especially medical researchers, public health officials, and health care delivery organizations, worry that overzealous or misdirected privacy protections could harm patient care and public health. They note that, despite the public worries illustrated in surveys, the vast majority of patients, when they are asked, agree to let their records be used for “legitimate” purposes, such as biomedical research approved by an IRB.<sup>29</sup> Similarly, the use of identifiable health information to protect the public, such as public health reporting requirements for communicable diseases, is well accepted.<sup>30, 31</sup> Furthermore, patients themselves may benefit when their caregivers have rapid access to relevant medical information in emergencies or when they can communicate with their caregivers electronically; and some advanced computerized medical information systems have been shown to reduce medical mistakes, lower costs, and improve overall quality of care.<sup>5</sup> <sup>22</sup> The cost of implementing certain privacy protections has also come under criticism,<sup>32</sup> as has their potential impact on, for example, employer-sponsored disease management programs.<sup>33</sup>

Each set of concerns has important implications, yet critical areas of agreement also exist. One area of agreement among all parties is that *the effectiveness of much of health care relies on patients' willingness to confide sensitive personal information to their caregivers.*<sup>20,34</sup> In the absence of open communication, ineffective care or worse could result. Indeed, most accept that the therapeutic bond of practitioners and patients relies on a profound trust, a critical building block of which is the patient's assumption of confidentiality.<sup>3,17</sup> (This concept is ancient: the Oath of Hippocrates states, in part, "Whatever I may see or hear in the lives of men which ought not to be spoken abroad I will not divulge.") Patients who doubt the confidentiality of the information they convey to clinicians and provider organizations may not tell practitioners all they need to know to make appropriate treatment recommendations; they may refuse potentially beneficial testing or treatment; they may ask practitioners to keep separate records, or not to report certain data; or they may even avoid care entirely. Unfortunately, patients have recently reported using all of these "privacy-protective" strategies in various settings,<sup>3,28,35,36</sup> which is of concern to all parties. Moreover, these concerns are heightened when patients' fears have proven to be justified. Anecdotes, and some data, exist of employers using health care data to make employment-related decisions<sup>31,37,38</sup> and of health care information being released inappropriately.<sup>39,40</sup> Identifiable patient data have been sold, bartered, and given away without patient consent for purposes as diverse as medical research, disease management programs, direct marketing campaigns, and by accident or malice.<sup>3,31,37,41-43</sup>

On the other hand, in some states where fairly strict privacy protections have been implemented, medical researchers, practitioners, and some of the public have balked at the restrictions.<sup>44</sup> It is possible that some types of legislation might lead to patients' family members being denied important information,<sup>45</sup> useful medical research being curtailed,<sup>29</sup> and significant costs being incurred.<sup>32,46</sup> There is thus a need for a balanced set of ethical norms regarding privacy and confidentiality protections for identifiable health information. This set of ethical norms should take into account the privacy concerns of patients, the social need for public health and safety protections, and the legitimate efficiency and quality concerns of patients, health care professionals, and other providers.

**Electronic Data Storage and Transmission.** Protection of informational privacy has taken on new urgency with the advent of electronic communications and record keeping, especially the use of the Internet.<sup>47</sup> *Electronic systems provide remarkable opportunities to protect sensitive information compared to paper records—through such mechanisms as user authentication protections, encryption technologies, and audit trails<sup>23-25</sup>—yet computerization may also allow quiet and rapid breaches of confidentiality,*

*potentially on massive scales.*<sup>23, 26, 37, 48-52</sup> Therefore, the desirability and feasibility of developing large data systems to improve research, monitoring, and quality have made developing strong privacy protections imperative today, so that appropriate research and quality improvement projects can move forward safely.

**Privacy: Ethical Background.** Individuals' interests in the confidentiality of their personal health information extends beyond their fears of losing health insurance or a job when this information is used inappropriately. Even in societies with universal health care coverage and strong antidiscrimination policies, the protection of health care records remains an important concern. This deeper (ie, not merely pragmatic) individual interest in informational privacy can be explained by two related ethical principles. Autonomy and fairness are two facets of an essential ethical concept that is often called "respect for persons." (Interestingly, each is also a core principle that underlies American democracy.) *Autonomy* requires that individuals be involved in decisions that affect their fundamental sense of personhood, or who they are and what they can do. Since dissemination and use of sensitive personal health information can fundamentally affect one's sense of self, and even one's life prospects, respect for autonomy demands that the individual's interests inform the access to or use of their personal information by others. Meanwhile, *fairness* is the core ethical principle that undergirds marketplace accountability. Among other things, it requires that individuals be given all the relevant information necessary to make important decisions—in colloquial terms, it is unfair to have to buy 'a pig in a poke.' Thus, for example, individuals should know the uses to which their information will be put before they can fairly be asked to decide whether to give the information to another. Fairness, like respect for autonomy, demands that anyone collecting or using sensitive personal information be concerned with the interests of the person whose information is at issue.

## Existing Community Norms/Standards

**The Fair Information Practices (FIP).** The content areas in this document have been strongly influenced by (although they are not precisely the same as) a list of principles known as “Fair Information Practices” (FIP). The FIP had their foundation in a 1973 report by the Department of Health, Education, and Welfare (HEW) Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens. The original FIP were as follows: (1) there must be no personal data record keeping systems whose very existence is secret; (2) there must be a way for individuals to find out what information about them is in a record and how it is used; (3) there must be a way for individuals to prevent information about them that was obtained for one purpose from being used or made available for other purposes without their consent; (4) there must be a way for individuals to correct or amend a record of identifiable information; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data. In 1974, the Privacy Act (5 U.S.C. §552a) became law in the United States. It is largely based upon the principles set out in the 1973 HEW report. Additionally, the FIP principles have been used by many European countries to form the basis of their own data protection laws.

**Organization for Economic Cooperation and Development (OECD) Guidelines.** The OECD Council issued its “Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data” in 1980. These guidelines, which the United States adopted on September 23, 1981, recognized that countries have a common interest in protecting privacy and individual liberty. The principles in this document fall into eight categories: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. These guidelines, while voluntary, constituted an effort toward harmonization across countries of information privacy protection rights and requirements.

**The European Union (EU) Directive.** Europeans and Canadians have sometimes used the term “data protection” to describe their informational privacy procedures, though slightly different approaches to data protection have been taken in Europe and in Canada. In October 1998, the EU Directive on the Protection of Personal Data went into effect. The Directive is the latest multinational policy document that codifies the concepts contained in the Fair Information Practices (now numbering eight, as noted above). It will require that non-EU countries have in place

“adequate” data protection mechanisms before receiving personal information from EU countries. It is possible, though by no means certain, that this could cause some personal information not to be sent to the US because the US lacks what the EU considers to be adequate data protections, particularly with regard to medical records.

**The Canadian Model Code.** In 1995 the Canadian Standards Association (CSA) issued its “Model Code for the Protection of Personal Information.” Modeled after the OECD Guidelines, it splits out two areas of special concern: consent, and the notion of ensuring organizations' compliance with the Code by appointing an accountable person within the organization.<sup>19</sup> The 10 principles in the CSA Code are as follows: (1) accountability; (2) identifying purposes; (3) consent; (4) limiting collection; (5) limiting use, disclosure, and retention; (6) accuracy; (7) safeguards; (8) openness; (9) individual access; and (10) challenging compliance.<sup>19</sup> Of note, the International Organization for Standardization (ISO) may consider adopting the CSA Model Code as an ISO standard.

**The Canadian Medical Association Code.** One purpose of the CSA Model Code was to allow different sectors of the economy to adapt the standards to their own specific needs.<sup>19</sup> The Canadian Medical Association (CMA) has done just that and issued their “Health Information Privacy Code” in August 1998. They have changed the wording of some of the principles from the CSA Code, but the underlying intent remains intact. The 10 principles contained in the CMA Code are: (1) the right of privacy; (2) special nature of health information; (3) constraints on purposes and limitations on collection, use, disclosure, and access; (4) knowledge and specification of purpose, collection, use, disclosure, and access; (5) consent; (6) individual access; (7) accurate recording of information; (8) security; (9) accountability; and (10) transparency and openness.

**Recent U.S. Legislative History.** In the United States, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) acknowledged the increasing computerization of medical information by codifying requirements for the electronic management of health information.<sup>53, 54</sup> Title II, Subtitle F of HIPAA is entitled “Administrative Simplification” and, in part, it calls on the Congress to pass legislation to protect the privacy of individually identifiable health information transmitted in connection with clinical encounters. The following are the major relevant provisions:

- Within 12 months of enactment (August 21, 1997), the Secretary of Health and Human Services must provide Congress with a set of detailed recommendations on standards to protect the privacy of individually identifiable health information. The recommendations must address rights individuals should have with respect to their information, procedures to exercise these rights, and

authorized/required uses and disclosures of the information. (The Secretary provided these recommendations to Congress in September 1997.)

- If the Congress has not acted on these recommendations within 36 months (by August 21, 1999), the Secretary of Health and Human Services must promulgate regulations to put protections in place within 42 months of enactment of the legislation (by February 21, 2000)—draft regulations to meet this requirement were circulated by the Secretary in October 1999.
- States that already have stricter laws than what is called for in this bill (with respect to confidentiality protections) are not required to relax their standards. In other words, HIPAA requires the establishment of a legislative floor, rather than a ceiling, for privacy protections.

In the 105th Congress, several legislative proposals were introduced, in both the House and the Senate, but none had bipartisan support. For example, the House passed a version of the “Patient Bill of Rights” that contained language on patient and medical record privacy and allowed nonconsensual use of identifiable data for “health plan operations,” but the bill was not acted upon in the Senate. The legislative futures of these various bills remain uncertain.

**Recent Private Sector Initiatives.** In addition to public sector initiatives (eg, the mandate for Congress or the Secretary of Health and Human Services to act, and activities taking place in numerous state legislatures), private sector organizations have been pursuing their own initiatives.<sup>33, 55-58</sup> These continuing efforts have been resulting in model legislation, organizational policy statements, and model policies and procedures. A few examples follow.

**Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and the National Committee for Quality Assurance (NCQA).** In late 1998, JCAHO and NCQA released a joint publication, *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment*.<sup>59</sup> The document makes several recommendations, addressing accountability; consent; educating patients and providers about privacy policies, procedures, rights, and responsibilities; technology; providing legislative support; and guiding research. Many of these recommendations are now making their way into accreditation standards.<sup>60</sup>

**The Model State Public Health Privacy Project.** This project is sponsored by the US Centers for Disease Control and Prevention, the Council of State and Territorial Epidemiologists, the Association of State and Territorial Health Officials, the National Conference of State Legislatures, and the Georgetown University Law Center (GULC). The purpose of the project is to create model state legislation for the privacy and security of public health

information. The latest draft of the model legislation was posted on February 19, 1999 (available at [www.critpath.org/msphpa/privacy.htm](http://www.critpath.org/msphpa/privacy.htm)).

**The Health Privacy Project.** Georgetown University’s Institute of Health Policy and Research is sponsoring several initiatives, such as the Health Privacy Working Group (HPWG). The HPWG sought to develop a set of principles for health privacy. Members of the Working Group represent disability and mental health advocates; health plans; providers; employers; standards and accreditation organizations; researchers; a pharmaceutical company; and experts in public health, medical ethics, information systems, and health policy. A report entitled *Best Principles for Health Privacy* was released recently,<sup>57</sup> and the Health Privacy Project has also prepared a practical, comprehensive guide to state health privacy laws.<sup>61</sup> More information on this project is available at [www.healthprivacy.org](http://www.healthprivacy.org).

**The National Association of Insurance Commissioners (NAIC).** In September 1998 NAIC adopted its Health Information Privacy Model Act.<sup>62</sup> This model for state legislation establishes standards to protect health information from unauthorized collection, use, and disclosure; establishes the right of an individual to examine his or her own protected health information; creates a limited right for individuals to have their protected health information amended or supplemented under certain circumstances; requires entities to establish procedures for safeguarding health information; and requires insurers to notify consumers about their privacy rights with respect to protected health information and how they may exercise those rights. The model bill applies to health information within the insurance industry only (more information available at [www.naic.org](http://www.naic.org)).

**American Medical Association (AMA).** The House of Delegates of the AMA in 1998 approved a new, more consolidated and comprehensive statement on patient privacy and medical records confidentiality (BoT Report 9, A-1998). Several unresolved issues listed in this policy were then referred to a Board/Inter-Council Task Force, including representatives from the AMA Board of Trustees and each of the AMA’s Councils. This task force has produced two sets of recommendations on these issues and on policy priorities for the AMA, which have been adopted by the AMA House of Delegates.<sup>63</sup>

**American Bar Association (ABA).** The ABA’s governing body adopted a recommendation in early 1999 urging that individuals have the right to prevent others from generating personally identifiable health information about them without their consent. The resolution favored the right to see, copy, and correct such information, and to bar disclosure absent “informed, voluntary, written” authorization by the individual. Additionally, the ABA established

the Electronic Communications and Privacy Interest Group under the ABA's Health Law Section to tackle legal issues surrounding electronic communication and privacy.

**American Association of Health Plans (AAHP).** In January 1999, as part of its "Putting Patients First" initiative, the AAHP revised its recommended member policies on the protection of patient privacy and record confidentiality.<sup>64</sup>

Numerous other organizations, including patient groups, physician and other professional associations, informatics and electronic data transmission associations, research organizations, managed care plans, and more, have recently revised, reconsidered, or created new privacy policies.<sup>33, 54, 56, 65-68</sup> Some of this activity can be traced to the recent US Congressional deadlines for action in this area, which spurred organizations to clarify their own policy priorities for health information privacy, but many documents from the United States and abroad also reflect fundamental concerns over how health care is adapting to the information revolution.<sup>47, 69</sup> And some research suggests that, although these issues have received a great deal of attention, uniform standards and practices to address them in the United States are not yet at hand.<sup>61, 70</sup>

## **E-Force: Measuring the Quality of Privacy and Confidentiality Protections**

One way in which the Ethical Force Program's work on privacy is distinct from that of other initiatives is that E-Force is interested both in discerning legitimate expectations for the protection of health information privacy and confidentiality and in developing valid, reliable, and feasible performance measures for the attainment of these expectations. Today, public demand, legislative deadlines, technological advances, and political pressure have coalesced to create a considerable interest in developing good performance measures for the protection of informational privacy and confidentiality in health care. Yet measuring the quality of privacy and confidentiality protections is difficult because numerous parties hold important stakes in the collection, storage, and use of health information. Each party may have different ethical standards, based on business, personal, professional, or public health ethics. Therefore, as in many important areas of health care quality, there is no single "gold standard" for measuring the quality of a party's policies and procedures to protect sensitive information.<sup>2</sup>

In areas of performance measurement where no clear gold standard exists, organizations interested in measuring quality (1) assess adherence to basic norms, (2) measure progress toward aspirational goals, and (3) suggest formal procedures to facilitate quality assurance and improvement in the area in question.<sup>2</sup> On the basis of reviews of the above codes and principles, as well as others, remarkable consensus has been noted around several themes,<sup>34</sup> suggesting that some widely accepted basic norms do exist—and these form the core of the expectations listed in this document. Aspirational goals were also widely expressed and found their way into some of the expectations, though it is recognized that sometimes they are very difficult to achieve. For example, they may be technologically challenging, or their achievement may be limited by attendance to other important social and ethical values. Finally, this report also suggests some formal mechanisms for ongoing assessment and improvement of privacy policies and procedures.

Most importantly, *the measurable expectations herein must be translated into specific measures—survey items, site review criteria, etc.—which then must be tested, validated, and approved by the E-Force Oversight Body before they will be released for use. Therefore, this document must be understood as being subject to revision.* We invite the readers' comments, criticisms, and constructive recommendations.

# Reading Notes

## How to Read This Document.

The format for each content area and associated set of measurable expectations is the following:

*Content area number* and a descriptive sentence or two *Rationale(s)* for the content area (one to four paragraphs)

*Table of general measurable expectations* for the content area that should be applicable to all parties to health care delivery. These are numbered 1.1, 1.2, 1.3, etc., and any necessary subcategories are lettered.

*Table of measurable expectations for specific parties* (if any) that apply only to specific parties in defined interactions. These are numbered 1.1s, 1.2s, 1.3s, etc.

*Explanations and exceptions* concerning the content area and its measurable expectations. These are bulleted and include important contextual comments and recommendations.

## Defining Terms.

Note that all terms that are italicized in the main body of the document are presented with specific definitions in the glossary. For ease of presentation however, not every word that appears in the glossary is italicized each time it appears. A few key definitions are below:

*Content areas* are general areas for development of performance measures within the domain of health informational privacy and confidentiality protections. They often cover many potential expectations for ethical action, only some of which may be measurable, and often include aspirational statements.

We often refer to certain uses of health information as being for the *direct therapeutic benefit* of the patient. This has sometimes been called the “primary” intended use of health information, since patients disclose sensitive personal information to clinicians and health care organizations for the purpose of their own therapeutic or diagnostic benefit. Nevertheless, it is difficult and perhaps impossible to separate every use of health information into “primary” or “nonprimary” categories. For example, labeling the use of information for payment as primary or nonprimary has been problematic. Nevertheless, when information is used for the direct therapeutic benefit of a patient, this frequently does not require additional explicit consent; consent may be inferred from the fact that the patient is seeking health care. Of course, some uses of health information that do not directly benefit the patient (ie, “nonprimary” uses) are extremely important. Medical research, public health research and practice, quality assurance and quality improvement projects, as well as billing and other health plan operations, accreditation

and licensure, etc., all may occasionally require the use of identifiable health information. That they are not directly of therapeutic benefit to the patient does not reduce their importance; it merely should raise the level of scrutiny they undergo before identifiable information is collected, stored, or used in their service.

*Health care delivery organizations* include all forms of organizations wherein patients receive health care. These need not include a physical plant per se, and will include practices without walls, independent provider associations, and preferred provider organizations, as well as other managed care organizations, hospitals, and all other institutional providers of health care.

A *health information trustee* is any person or organization in whom protected health information is entrusted. Trustees may have protected information entrusted to them by individuals, or they may receive information from another source, such as another trustee or through their access to laboratory studies, prescription records, etc.

Where *individuals* are mentioned, authorized guardians of individuals (such as the parents of minors) should be included where the sense allows.

*Measurable expectations* will be the targets of specific performance measures. They are potentially measurable areas within each content area, as defined by the existence of an explicit expectation for ethical action, with the corresponding possibility that one could measure achievement of the expectation in a reliable and valid way.

*Protected health information* includes all personally identifiable information about health care conditions, diagnoses, or treatments. It comes in many formats and from many sources. For example, protected health information may be in the form of lab studies, human tissue, a clinician's notes, or any other part of a patient record (see Record, below).

*The purchaser* is the entity or individual responsible for buying health care or a health insurance policy for an individual or group, including self-insured employers contracting with care delivery organizations.

*The record* is the data pertaining to direct clinical care that are held by a health information trustee; used synonymously with “clinical record” or “chart.”

# Content Areas and Associated Measurable Elements for the Protection of Privacy in Health Care

## Area 1. Transparency

Health information trustees should make publicly available clear explanations of their policies, procedures, and practices regarding the collection, storage, and use of *personally identifiable health information*.

### Rationales

First, respect for persons demands that individuals must have the relevant information to make informed decisions about when, how often, how much, and what type of identifiable health information to confide to others. In the therapeutic context, patients generally agree to confide sensitive information to clinicians and health plans on the presumption that the information is necessary for the purposes of their own care. If the information is to be used for other than the patient's direct diagnostic or therapeutic benefit, whenever possible the patient should know this before the information is collected. Second, if an organization fails to disclose its policies and practices regarding the privacy, security, and confidentiality of the personally identifiable health information entrusted to its care, patients may assume the worst and choose not to disclose all of the information necessary for optimal care. For example, fear of disclosure of sensitive health information to employers may rise when employers' privacy policies are not known, leading some patients to forgo useful testing or treatment offered by their employers. Third, this same fear of unauthorized disclosure could also lead to suboptimal organizational functioning if individuals hold back information that is useful for organizational operations. Fourth, and perhaps most important, information trustees, knowing that their policies and the rationales for these policies will be open to scrutiny, will consider carefully what those policies should be. That is, there is some benefit that derives merely from careful consideration in the process of developing policies. Therefore, even if few individuals avail themselves of the opportunity to learn about an organization's policies and practices, which may be quite complex, the fact of their ability to do so can serve a useful purpose.

The complexity of privacy and confidentiality protections in the evolving health care system demands that the process of transparency should involve the ongoing and coordinated efforts of numerous health information trustees, including

employer/purchasers, health care delivery organizations, practitioners, and others. For example, purchasers, such as employers, might well help health plans to explain and publicize that patients/beneficiaries have the right to access and copy their health care *records*. The following are potentially measurable expectations that apply to health information trustees, and around which specific performance measures will be developed and tested.

### Measurable Expectations

**General expectations:** Performance measures for the following will be developed for all parties in health care delivery.

1.1 The health information trustee makes publicly available, in clear and understandable language, general descriptions of its policies and practices regarding the collection, storage and use of identifiable health care information.

Policies disclosed include:

- a) Classifications of who will have access to the information collected
  - b) What general measures are used to protect the security of health information
  - c) Under what sorts of circumstances personally identifiable information might be used or accessed without the individual's consent for nontherapeutic purposes
  - d) How the integrity and quality of the data will be ensured
  - e) The procedures through which individuals may obtain access to their own identifiable health information
  - f) The procedures through which individuals may suggest amendments to be appended to their record(s)
  - g) Any rights of redress an individual has to address breaches of privacy, security, and confidentiality policies
  - h) What/who is/are the organizational point(s) of contact for privacy, security, and confidentiality concerns
  - i) In general, how long identifiable information will be held, including general descriptions of organizational policies on data destruction and de-identification
- 1.2 The information in 1.1 is periodically updated and redistributed. If significant changes occur in policies or procedures, especially any changes that could result in nonconsensual accessing, disclosure, or use of personally identifiable health information, relevant parties are notified of such a change.

**Expectations for specific parties:** *Performance measures for the following will be developed only for certain relevant parties.*

1.1s Health care delivery organizations make available to clinicians, who collect and maintain records of personally identifiable health information, information on policies and procedures regarding the potential or actual use of this information for any purposes other than direct clinical care. This includes generally when such information may be used without patient consent.

## **Area 2. Consent**

Whenever feasible, health information trustees should obtain valid informed consent from individuals for the collection, storage, or use of personally identifiable health information. If consent is not obtained, then a formal, authoritative, and publicly accountable process must be used to authorize a waiver of consent.

### ***Rationales***

With an individual's valid informed consent, almost any use of identifiable health information is allowable, and this is justifiable on the basis of individual autonomy. Conversely, of course, denial of consent should also be respected. Respect for persons requires that patients and others have the right to decide when and with whom they will share their sensitive health information and for what purposes. In addition, except in very constrained circumstances, such as where public health and safety are concerned, a right to consent to the collection, storage, and use of personally identifiable health information is crucial to maintain trust in the health care delivery system. Without trust, patients and others will be less likely to confide information necessary for health care purposes.

The measurable expectations below are concerned first with ensuring that valid informed consent is obtained whenever it is feasible to do so. As important as this is, it is not always possible or feasible to obtain valid informed consent for every legitimate use of identifiable health information. The elements below then call for the implementation of formal, authoritative, and publicly accountable procedures to justify and authorize the collection, storage, and use of protected health information without consent. That is, a legitimate process should be followed to authorize the waiver of the informed consent requirement (others have called this process "substituted consent"). This process can help to ensure that protected health information that is collected, stored, or used without valid consent is necessary for an important and legitimate purpose; the minimal information necessary for the purpose; minimally identified; and used only for authorized purposes (see also Content Areas 3 and 7).

One possible explicit, formal, and open process to authorize the use of identifiable information without patient consent is defined in some detail below and in Appendix 1—the data disclosure board. (This name has been taken from a document created by the NCQA and JCAHO.<sup>54</sup>) While the data disclosure board (DDB) has some features and duties reminiscent of an institutional review board (IRB), and some reminiscent of hospital or health plan medical records or patient privacy committees, it is not quite any of these - though in some organizations it will be possible for an existing entity to take on the described roles of the DDB (see Appendix 1). What is crucial is that, whatever the name of the entity performing this role, it should undertake careful deliberations based on the important considerations noted—especially the evaluation of specific documents describing the need for the data and the impact of the collection, storage, and use of the data on privacy. This is to ensure that every activity wherein identifiable patient records are accessed or used without patient consent will receive accountable oversight. (Appendix 1 includes a table describing the sorts of activities that might require this DDB-type oversight vs. IRB or other sorts of oversight.)

Finally, of note is that consent for the use of information for the direct therapeutic benefit of the patient may generally be inferred from the fact that the patient presents for care. However, in some circumstances the patient may legitimately request that therapeutic or diagnostic uses of information be constrained. That is, fully informed and competent patients should be allowed to opt out of even personally beneficial uses of their own identifiable health information whenever this is feasible. Health information trustees should clearly define situations where this is not the case. Similarly, use of some information for payment purposes may be presumed from the fact that the patient submits a bill for reimbursement. Yet, for example, private payment for services (ie, no charge made to an insurer) should confer on patients the right to withhold information about these services from others.

### ***Measurable Expectations***

**General expectations:** *Performance measures for the following will be developed for all parties in health care delivery.*

#### **Valid Informed Consent**

2.1 Valid informed consent for collection, storage, and use of identifiable health information includes disclosure of all necessary information that a reasonable person would use in making an informed decision, in a format that is readily understandable to the individual, and without coercion influencing choice. The information conveyed includes the information described in Measure 1.1 (a-i).

## Process for Waiver of Informed Consent

- 2.2 Valid informed consent to the collection, storage, or use of personally identifiable health information is required, unless its waiver has been justified and authorized by an explicit formal mechanism that is publicly accountable.
- 2.3 Health information trustees that collect, hold, disclose, access, or use personally identifiable health information without the valid informed consent of the subjects of the information (and not in the course of medical research covered by the Common Rule or in the course of legal obligations) have in place a formal, authoritative, and publicly accountable process to address the necessity of doing so (such as the Data Disclosure Board described in Appendix 1).
- 2.4 Written records are kept of the proceedings and decisions from this process.

## Documentation of the Process

- 2.5 The process includes the careful review of a data needs assessment (DNA) document, submitted by the data requestor, for any nonconsensual use of personally identifiable health information. A written DNA addresses the legitimate need for information to be collected, stored, or used without valid consent (see Explanation and exceptions below).
- 2.6 The process includes the careful review of a written privacy impact assessment (PIA) document, submitted by the data requestor, for any nonconsensual use of personally identifiable health information. A written PIA addresses the risks and benefits, to patients, beneficiaries, employees, and other stakeholders, of the proposed collection, storage, and use of identifiable information without valid consent (see Explanation and exceptions below).

## Opt-Out Provisions

- 2.7 Patients are allowed to deny the release of their identifiable health information *outside* the organization receiving the information, except as required by law or as approved through a formal authorization process that is publicly accountable.
- 2.8 The health information trustee has clear and public policies on what uses of health information are not optional.

**Expectations for specific parties:** *Performance measures for the following will be developed only for certain relevant parties.*

- 2.1s Health care delivery organizations have specific policies that address under what circumstances and how informed consent is or is not obtained for the use of identifiable health information in QA/QI projects.

- 2.2s Consents for release of identifiable beneficiary health information to employer-purchasers or for any commercial uses of the information are separate from other consent processes.
- 2.3s Enrollment consent forms cover only known and routine needs for the use of the patient's identifiable health information. General consent on entry into a health care delivery organization may include the use of identifiable information for treatment, coordination of care, billing, fraud detection, and specific and known oversights reviews, such as by the Health Care Financing Administration, states, and accreditors, or public health purposes that are required by law.

## Explanation and exceptions

- *The data disclosure board:* We have used the term “data disclosure board” to describe one type of formal, authoritative, and publicly accountable mechanism to provide a standard minimal level of oversight to certain activities involving the use of identifiable health information without consent, some of which receive little or no formal review today. In many organizations existing committees already perform some or all of the described functions—such as a medical records committee or a privacy policies committee. Such existing committees, regardless their names, may be most readily adapted to achieve the suggested roles of the DDB.
- *Institutional review boards:* Note that the use of identifiable health information for research that is covered by the Common Rule (45 CFR, Part 46) does not require additional oversight beyond that provided by the IRB.
- An informed observer, after reading *the data needs assessment document*, should be able to answer questions such as the following:
  - Must the individual's privacy interests be compromised because a legitimate secondary purpose could not practically be served if consent were required?
  - Is the purpose to be served publicly available?
  - Is the least intrusive means feasible to be used to collect the information?
  - Is the most complete notice feasible to be made to the persons whose information is involved?
  - Will any proposed nonconsensual collection and use of information foreseeably intrude upon collection or use of information for direct therapeutic purposes?
- An informed observer, after reading *the privacy impact assessment document*, should be able to answer questions such as the following:

Will all reasonable steps be taken to ensure that the least identifiable (that is, the most difficult to link to an individual) information is used that is consistent with the stated purpose?

Might the potential or real vulnerability of patients be exploited in collecting or using the information?

Might patients' direct care be negatively affected?

- **Small practices:** Some small organizations and individual health information trustees may only infrequently use identifiable health information for other than routine therapeutic and quality assessment/quality improvement activities. Acceptable mechanisms to fulfill the requirements of a formal, authoritative, and publicly accountable review process for such entities include (1) grouping together with other organizations to create a review committee and provide peer oversight; (2) formally adopting and utilizing standard practices and policies that are developed nationally, regionally, or by a health care delivery organization with which the organization contracts; and/or (3) avoiding the use of patient-identifiable information for nontherapeutic purposes unless specific informed consent is obtained.
- **Emergencies:** In rare circumstances it will not be possible to obtain either valid consent or a complete review of a request for an urgent use of health information, such as in some outbreak investigations or other urgent or emergency situations. A rapid review function will ameliorate such situations but may not eliminate them. When such situations dictate the rapid nonconsensual use of identifiable information, a formal retrospective review of the situation should be undertaken later.
- **Law enforcement:** In some circumstances, authorization to access identifiable information is given by a legal authority other than the individual originator of the information at issue. One example is the use of identifiable health information for law enforcement activities. Law enforcement access to personally identifiable health information should operate under the same principles as law enforcement access to other sensitive personal property and information. Access should require probable cause and a court order, unless it occurs in "hot pursuit" of a crime. In addition, when health information is used for a previously unauthorized use solely on the authorization of a legal authority, the remainder of these principles should be followed to the extent possible. For example, the least intrusive information, the least identifiable information, released to the fewest number of people, and held for the shortest necessary period of time, should be collected or accessed and used. The equivalent of *data needs and privacy impact assessments* should be completed as far as is practical. The results of these assessments should

be conveyed in writing to the legal authority that is requesting the information. Written notice should be given to the legal authority to (a) note the protected and sensitive nature of the data that is being disclosed; (b) request disclosure of the least intrusive data possible; (c) request that the legal authority adhere to these standards in its storage, redisclosure, and use of the data; and (d) request that the legal authority either return the data or destroy it when it is no longer useful for the authorized purpose (see also Content Area 8, Accountability).

### **Area 3. Collection Limitation**

Health information trustees should limit collection of health information to that information required for current needs, or reasonably projected future needs, which are made explicit at the time consent is obtained.

#### **Rationales**

Even in the setting of informed consent, information collection should be limited by reasonably expected and explicit uses of the information for several reasons. First, information to be used in some vague future circumstance should not be collected or stored because this poses unnecessary risks to the patient's privacy. Second, individuals who are asked to provide information that appears to be irrelevant to stated purposes may develop concerns that the information is intended for unauthorized and hidden purposes. This could lead them to become reticent, or less than fully honest, in discussing/disclosing sensitive information as a way to protect themselves from unknown and unauthorized uses of their information. Worse yet, patients could postpone needed care, or mislead practitioners as to their symptoms or health care needs. Health information trustees will obtain better and more complete data from individuals when the individuals are assured that the information they provide will not be used for other than stated and authorized purposes. Finally, as noted above, for consent to the giving of information to be valid it must include notice of all intended uses of the information to be gathered.

## Measurable Expectations

**General Expectations:** *Performance measures for the following will be developed for all parties in health care delivery.*

- 3.1 All data collectors receive training in collection limitations, including fair and lawful means to collect information and the rationales for limiting data collection.
- 3.2 The health information trustee has a written policy on health information retention and destruction that specifies whether and how identifiable health information that is not reasonably expected to be used for one or more defined purposes is to be discarded, de-identified, or archived.

## Explanation and exceptions

- *The training of individuals* who are charged with collecting, storing, and using identifiable health information, including clinicians, administrators, and billing personnel, should include information such as the following:

Health information trustees should collect and maintain only that identifiable health information that is necessary for the patient's care and other authorized purposes

The process(es) by which authorization for waivers of informed consent may be obtained

The definition of informed consent

What information is "personally identifiable"

That clinicians, when acting in their role as caregivers and patient advocates, should not collect information that is not relevant, in the clinician's professional judgment, to the direct therapeutic or diagnostic benefit of the patient

When patients go outside of a health plan and pay out of pocket for care, information about this care is not released to the health plan or others except with the consent of the patient or as required by law.

## Area 4. Security

Health information trustees should protect the identifiable health information in their care by using reasonable security measures appropriate to the sensitivity of the information. A specific individual or group should be identified as being responsible for overall security mechanisms and processes.

## Rationales

Individuals are reasonably entitled to demand stringent security measures for their personally identifiable health information. Breaches of the security of personally identifiable health information are breaches of trust. Moreover, though the risk of unauthorized access, use, or modification of data may be difficult to quantify, the potential harms are grave. And merely the perception that security measures to protect sensitive information are inadequate may be enough for patients to give inaccurate or incomplete information in an effort to protect themselves from unauthorized uses of their personal information. Effective security measures can thus reassure patients that their personal information will be safe, which will improve data collection and hence patient care, public health, and organizational functioning.

## Measurable Expectations

**General expectations:** *Performance measures for the following will be developed for all parties in health care delivery.*

### Written Policies

- 4.1 Health information trustees have written policies that delineate the security measures used to protect identifiable records from risks such as loss, or unauthorized access, destruction, use, modification, or disclosure.

### Security of information stored and transmitted on paper

- 4.2 Health information trustees have physical security measures in place where paper records are used to ensure that:
  - a) Areas where health information is stored physically (eg, record rooms, file cabinets, etc.) are locked when not attended
  - b) There is a mechanism to sign out and track the whereabouts of physical records
  - c) A record is maintained to track instances where clinical records are copied and distributed
  - d) Identifiable health information is not visible in public areas (see "Explanation and exceptions" below)

### Security of information stored and transmitted electronically

- 4.3 Health information trustees have electronic security measures in place where electronic records are used, to ensure that:
- a) Identifiable data is encrypted for any external transfer over the Internet
  - b) Automated access controls and user profiles are in place in any computer or computer system storing identifiable medical information
  - c) User-friendly audit trails are in use and checked regularly or randomly
  - d) User authentication protections are in place (eg, secret passwords or biometric identifiers)
  - e) Identifiable health information visible on computer screens is not easily read by public passersby and computer screens are disabled when the user leaves his/her computer terminal.

**Security Officer or Team**

- 4.4 Organizations that are health information trustees designate one or more specific individuals to be accountable for overall security measures, regular review of security issues, and updating of security protocols (eg, a security officer or team).
- 4.5 The security officer, or other responsible party, does the following:
- a) Performs or supervises periodic audits of health information security procedures to detect and prevent breaches in security
  - b) Defines and periodically updates mechanical and electronic de-identification procedures and oversees their use

***Explanation and exceptions***

*Identifying patients in clinical settings:* When a patient receives care in a clinic, emergency room, or hospital unit, it is sometimes not possible to entirely mask who the patient is and why he or she is there. For example, a patient on an Alzheimer's disease unit might need to have his name on his room door to help him find his way back to the room, which would necessarily place his name in a public area where his diagnosis could easily be inferred. In general, it is more acceptable to breach privacy in such situations when this is of direct and primary benefit to the patient, or when it is necessary to prevent harm to others (as when a patient endangers others through a credible threat of violence). When cases of this sort arise, the health information trustee should have a written policy explaining the rationale for breaching privacy in each class of such cases. The trustee might charge the body responsible for reviewing privacy impact assessments (eg, DDB) with reviewing and providing justifications for these classes of cases.

**Area 5. Individual Access**

Individuals should be allowed access to view and add information to their personally identifiable health information records.

***Rationales***

First, an individual's interest in informational privacy includes the concept of the legitimacy of his or her continued control over information that the individual has chosen to confide. Individuals maintain a very strong interest in the accuracy of their health care information, even after giving it to a health care entity in hopes of serving their health needs. Individuals should have a right to see that the recording of their information is accurate and reflects what they intended to impart. Other health information may derive from medical testing, where the patient has less control over how much and what type of information is collected. However, having some knowledge of and control over this information may be vitally important to the patient's life plans and ability to make informed choices, which is critical to individual autonomy. Therefore, patients ought to be able to know about all of their health care information held by a trustee.

Second, the principle of consent requires that the patient understand what he or she is consenting to. A full understanding of the contents of one's health records is necessary before informed consent to the release and use of these records can occur. Similarly, one must know to whom one is entrusting information. Therefore, as far as it is feasible, health information trustees should allow individuals to know who has gained access to their personally identifiable information and for what purpose(s).

***Measurable Expectations***

**General expectations:** *Performance measures for the following will be developed for all parties in health care delivery.*

- 5.1 Except in very limited circumstances (see "Explanation and exceptions" below), the health information trustee provides individuals access to review and copy their own identifiable health information.
- 5.2 Should patients review their information and believe it to be incomplete or inaccurate, health information trustees allow individuals to suggest amendments, which will be appended to their records. There need not be a requirement to delete data that are inaccurate or incomplete; rather, corrected information may be added to the record with the date and source of the appended information marked.

**Expectations for specific parties:** *Performance measures for the following will be developed only for certain relevant parties.*

5.1s Health care delivery organizations inform clinicians of relevant policies that allow patients access to copy and amend medical records that are maintained by the clinicians.

### ***Explanation and exceptions***

***“Therapeutic privilege”:*** In very rare circumstances, information about a patient’s health care or health status may temporarily be withheld from the patient by clinicians if, in their professional judgment, there appears to be a significant risk of substantial harm to the patient or others that would be expected if immediate access were granted. This is one sort of what has been called the clinician’s “therapeutic privilege.” Of note, a health care professional can justify withholding information from patients only on the basis of direct therapeutic benefit to the patient involved, or because of a significant risk to identifiable others. Even in these rare cases, temporizing measures, such as requesting that a patient wait a few days for a “cooling off” period, are typically more appropriate than would be complete secrecy regarding the contents of the patient’s records.

***Legal requirements:*** Exceptions to patients’ access to their records may rarely occur because of legal requirements, as when information is held under court seal, when a confidential source of information exists, when the data contain information about other individuals (other than health professionals), or when adolescents, younger minors, or guardianships are involved. As a general rule, if information is being disclosed to a third party, then it should also be disclosed to the subject of the information except in cases of endangerment.

***Information in transit:*** Some entities, such as Internet service providers for health care delivery organizations, serve only as information conduits and do not otherwise maintain, store, or use identifiable health information. These entities are, very briefly, entrusted with health information, but as long as they do not store, access, or use the information themselves, they are responsible only for security measures and the safety of the information as it transits their system. They should not need to create special mechanisms to oversee other uses of this information, such as creating mechanisms for individuals to view or amend their records.

## **Area 6. Data Quality**

Health information trustees should seek to ensure that the identifiable health information in their care is as accurate, complete, and up to date as is required for the purposes for which it is collected and used.

### ***Rationale***

First, health care information must be both accurate and timely to ensure its effectiveness. Accuracy of health information is crucial for therapeutic purposes, and even accurate information that arrives too late may be of no therapeutic use. Second, inaccurate information can potentially distort justice and equity in the health care delivery system by inappropriately diverting resources away from important needs (for instance, if one patient’s need for an organ is inaccurately exaggerated, another patient may unfairly be denied the organ). Finally, inaccurate information could also impair an individual’s privacy interests in unpredictable and distressing ways, such as if an incorrect diagnosis is attached to a patient’s records, which could force the patient to disclose other records to prove its inaccuracy.

### ***Measurable Expectations***

**General expectations:** *Performance measures for the following will be developed for all parties in health care delivery.*

- 6.1 Health information trustees perform periodic audits to ensure the accuracy of identifiable health data.
- 6.2 Health information trustees regularly review and evaluate their security and confidentiality measures to ensure that they do not unduly interfere in the timely and accurate transmission and receipt of information necessary for patient care.

## **Area 7. Information Use Limitation**

Health information trustees should limit the disclosure and use of personally identifiable health information to those purposes that are made explicit at the time consent is obtained or are otherwise authorized through a formal, authoritative, and publicly accountable mechanism.

### ***Rationale***

First, for patients the assumed primary purpose for disclosing personal health information to others is to obtain some personal diagnostic or therapeutic benefit. Thus, insofar as any subsequent use of the information they disclose is solely for their personal therapeutic benefit, no further consent or notice is routinely required on the part

of health information trustees. However, the disclosure or use of this information for other purposes will require the individual's consent, or else some special justification and authorization. Any use of health information that has been confided for one purpose to fulfill another purpose, if done without consent, is a breach of the individual's interest in maintaining his or her informational privacy, which can put at risk both the individual's personal dignity and his or her trust in the health information trustee. Such breaches must therefore be justified through an accountable waiver of consent process as described above. As with the principle of consent above, primary concerns for these measures are to ensure that nonconsensual uses of identifiable health information are formally justified and limited such that they do not (1) exploit patient vulnerability; (2) inhibit patients from confiding information necessary for their own therapeutic benefit; or (3) otherwise impede the collection, storage, or use of information for authorized purposes.

Second, valid informed consent to the use of identifiable health information for nontherapeutic purposes is difficult to obtain, since it is hard to avoid subtly trading on the patient's trust in his/her clinicians or the health care organization. This is because patients generally will provide health care practitioners with requested information on the assumption that it is necessary for their own health care. Even if told that the information requested is not for their immediate needs, they are likely to disclose it to health care practitioners, if only to preserve relationships. Hence, any nontherapeutic uses of identifiable health information should be especially closely constrained by formal processes to ensure that attention is paid to the risks and benefits of collecting and using identifiable information for these purposes.

### *Measurable Expectations*

**General expectations:** *Performance measures for the following will be developed for all parties in health care delivery.*

- 7.1 Identifiable information that is collected for a defined purpose is not used for another purpose without explicit consent, unless legally required or else authorized through a process allowing waivers of consent for the use of health information (such as a DDB).
- 7.2 Access privileges among individual employees and contractors of a health information trustee are directly tied to the necessity of access to the information for the individuals' job functions.

- 7.3 There is no commercialization (sale or exchange for commercial purposes) of identifiable health information without the informed consent of the individuals whose information is involved.
- 7.4 Health information trustees have in place written policies that describe the circumstances and documentation necessary to authorize the release of identifiable health information to law enforcement officials (see also "Explanation and exceptions" below, and under the principle of consent above).
- 7.5 When a patient's identifiable health information is subpoenaed, the trustee notifies the patient with as much advance notice as can reasonably be given.

**Expectations for specific parties:** *Performance measures for the following will be developed only for certain relevant parties.*

- 7.1s Employer/purchasers have a written policy that they will not use employees' identifiable health information for making employment-related decisions.
- 7.2s Employer/purchasers have a written policy that only specific individuals responsible for administering health plan benefits have access to identifiable health information.
- 7.3s Researchers do not report data in a way that makes it feasible to infer the identity of individuals.
- 7.4s As applicable, health care delivery organizations have written policies, which are updated periodically, stating:
  - a) That only aggregate data/statistics will be released to employers about the utilization of benefits by their employees
  - b) The process to decide when patient information may be used in biomedical research without valid consent
  - c) The process for blinding of data, including the plan's definition of "de-identified data" for specified uses, and how de-identification is to be achieved
  - d) The process for review of outside requests for identifiable health information, including for research, accreditation, licensure, and quality assurance
- 7.5s When organizations such as accrediting bodies, purchasers, law enforcement agencies such as courts, and others gain possession of identifiable health information, they become health information trustees, and attend to protected health information in the same manner as other health information trustees regarding the collection, storage, and further disclosure or use of the information in their possession.

### ***Explanation and exceptions:***

*Law enforcement:* When required by law, a health information trustee may be forced to relinquish identifiable health information despite a negative privacy impact review by its formal internal review process, or without adequate time to conduct such a review. When responding to such legal mandates, data should be disclosed including a cover letter providing notice as to the protected nature of the data (other details on the contents of such a notice are described under the “Explanation and exceptions” bullets in Area 2, Consent, above).

## **Area 8. Accountability**

Health information trustees should be accountable for adhering to standards for the collection, storage, and use of personally identifiable health information, including the responsible transfer of information to other accountable information trustees.

### ***Rationale***

Protection of health care informational privacy involves different types of accountability for a wide array of parties, on a variety of topics related to the collection, storage, and use of personally identifiable health information. Moreover, accountability for protecting identifiable health information occurs through various mechanisms. It can occur through socialization to community norms (by informing trustees about expectations, for example) as well as through other private and public sector activities. In the end, using a variety of forms and mechanisms of accountability, it is important to enforce similarly high levels of accountability for the care of personally identifiable health information among all health information trustees. As health care information passes from one person or organization to another, any lapses of accountability could have dramatic consequences for all. Failure in any part of this “chain of accountability” could lead to individuals choosing not to confide information to other links in the chain, making the responsibility and efforts of all other parties moot, and hindering health care delivery. For this reason, unauthorized access to, disclosure of, or use of personally identifiable health information should lead to commensurate and consistent disciplinary actions regardless the status or type of the offending party.

### ***Measurable Expectations***

**General expectations:** *Performance measures for the following will be developed for all parties in health care delivery.*

- 8.1 Health information trustees furnish clear policies and materials to all of their agents who have access to identifiable health information to support their training in the proper handling of sensitive health information.
- 8.2 Health information trustees ensure that individuals handling identifiable health information are properly trained, on a regular basis, in their security and confidentiality standards, including requirements that are specific to each individual’s job.
- 8.3 Reprimands, feedback, education, probation, and other appropriate methods are used to enforce adherence to privacy and confidentiality protection standards.
- 8.4 Written policies specify what level of penalty will result from specific breaches of privacy and confidentiality protections.
- 8.5 Individuals handling, or with access to, identifiable health information display knowledge of protections afforded this information and the penalties associated with breaching the security or confidentiality of this information.
- 8.6 Health information trustees have in place a formal internal mechanism for individuals to bring forth, without fear of reprisal, complaints of inappropriate collection, storage, or use of personally identifiable health information.
- 8.7 When an internal review mechanism does not provide a satisfactory resolution, there is an opportunity for external review of unresolved privacy complaints.
- 8.8 Health information trustees, unless otherwise prevented by law, require a written statement of adherence to privacy, security, and confidentiality standards from all employees, agents, subcontractors, and outside organizations who wish to gain access to protected health information.

### ***Explanation and exceptions***

*Using contracts to create seamless health information protections:* Health information trustees must be accountable for their own attention to the protection of individuals’ privacy interests, but the system of privacy protections will not be effective if information transferred outside a responsible trustee does not receive continuing protection. Ensuring this continuing protection is partially the responsibility of the trustee transferring the information. As noted above (8.8), meeting this obligation will be facilitated by ensuring that entities receiving information from health information trustees must contractually promise to adhere to specific standards.

# Glossary

**Clinician:** Any person who delivers health care services to patients.

**Consent:** Valid informed consent for the collection, storage and/or use of identifiable health information includes the disclosure of all necessary information that a reasonable person would use in making an informed decision, in a format that is readily understandable to the individual, and without coercion influencing choice (for further details on what should be conveyed to obtain valid informed consent, with regard to primary concerns, see Elements 1.1 a-i and 2.1).

**Direct therapeutic benefit:** This document refers to certain uses of health information as being for the direct therapeutic benefit of the patient. For example, sharing information between two clinicians caring for the same patient is generally of direct benefit. This has sometimes been called the “primary” intended use of health information, since patients disclose sensitive personal information to clinicians and health care organizations for the purpose of their own therapeutic or diagnostic benefit. Nevertheless, it is difficult and perhaps impossible to separate every use of health information into “primary” or “nonprimary” categories. For example, labeling the use of information for payment as primary or nonprimary has been problematic. Nevertheless, when information is used clearly for the direct therapeutic benefit of a patient, this frequently does not require additional explicit consent; consent may be inferred from the fact that the patient is seeking health care. Of course, some uses of health information that do not directly benefit the patient (ie, “nonprimary” uses) are extremely important. Medical research, public health research and practice, quality assurance and quality improvement projects, as well as billing and other health plan operations, accreditation and licensure, etc., all may occasionally require the use of identifiable health information. That they are not directly of therapeutic benefit to the patient does not reduce their importance; it merely should raise the level of scrutiny they undergo before identifiable information is collected, stored, or used in their service.

**Health care delivery organizations:** All forms of organizations wherein patients receive health care. These need not include a physical plant per se, and include practices without walls, independent provider associations, and preferred provider organizations, as well as other managed care organizations, hospitals, and all other institutional providers of health care. Financing care (an insurance function) may or may not be a function of a health care delivery organization.

**Health information:** Information that contains health status, treatment history, or diagnoses.

**Health information trustee:** Any person or organization in whom protected health information is entrusted for collection, storage, or use. Trustees may have protected information entrusted to them by individuals, or they may receive information from another source, such as another trustee or through their access to laboratory studies, prescription records, etc.

**Identifiable health information:** Health information is always identifiable if it contains the originator’s name, address, telephone number, or Social Security number, or has readily available links to such information. However, virtually any data set, in the right hands, can be used to identify at least some individuals. An appropriate definition of “identifiable” should thus vary based on both the user and the use proposed. Health information trustees should define, with periodic updates, what degree of de-identification of data they consider sufficient for defined purposes, and what procedures they use to de-identify data (see also Security measure 4.5).

**Individuals:** In this document, where individuals are mentioned, authorized guardians of individuals (such as the parents of minors) should be included where the sense allows.

**Protected health information:** All personally identifiable information about health care conditions, diagnoses, or treatments, which may come in many formats and from many sources. For example, protected health information may be in the form of laboratory studies, human tissue, a clinician’s notes or any other part of a patient record (see Record, below).

**Purchaser:** The entity or individual responsible for buying health care or a health insurance policy for an individual or group, including self-insured employers contracting with care delivery organizations.

**Quality assurance/quality improvement (QA/QI):** QA/QI activities are intended to directly assess and/or improve the quality of health care delivered. These activities may or may not have as one goal the production of broadly generalizable new knowledge.

**Record:** Data pertaining to direct clinical care that are held by a health information trustee; used synonymously with “clinical record” or “chart.”

# Appendix 1

## *Some Notes on the “Data Disclosure Board”*

One possible explicit, formal, authoritative, and open process to authorize the use of identifiable information without patient consent is to use a publicly accountable oversight committee, which we have called a data disclosure board (DDB). This name was suggested in a document created by the NCOA and JCAHO,<sup>71</sup> but the name is much less important than the function of this proposed entity. Others have suggested and implemented similar entities under other names.<sup>72</sup> It is worthwhile noting that, while the DDB has some features and duties reminiscent of an institutional review board (IRB), and some reminiscent of hospital or health plan medical records or patient privacy committees, its function is not exactly the same as any of these—though in some organizations it will be possible for an existing entity to take on the described roles of the DDB. What is crucial is that, whatever the name of the entity performing this role, it must undertake careful deliberations based on the important considerations noted—such as the evaluation of explicit *data needs* and *privacy impact assessment* documents—and it must be publicly accountable for its decisions. The purpose of the DDB is to ensure that every activity wherein *identifiable* patient records are accessed or used *without patient consent* receives a standard level of legitimate and accountable oversight—as all research projects covered by the Common Rule (CFR 45 Part 46) currently do. See the Table for a suggested list of the sorts of activities that might require DDB-type oversight vs. IRB or other sorts of oversight. The Ethical Force Program hopes to encourage local variation and testing of the implementation of the DDB concept, which will be necessary for its effective functioning in a wide variety of situations.

The DDB concept is designed to fill an accountability gap. At the present time, many uses of identifiable health information both within and outside the health care system, which are often legitimate, receive no regular formal oversight.<sup>73</sup> This is generally the case for those uses of information listed in the table as being appropriate for DDB oversight.

Note that the DDB is intended to review only uses of *identifiable* health information (“identifiable” is to be defined, if necessary on a case-by-case basis, by the health information trustee) and only *when valid informed consent will not be obtained* (see Figure on p. 8).

Small group and solo health care practitioners, among other small organizations, may find the concept of creating a formal accountable oversight mechanism to evaluate uses of identifiable health information without patient consent impractical. For this reason, such organizations may choose to (1) join together with other organizations to create a shared review committee; (2) formally adopt and utilize standard practices and policies that are developed nationally, regionally, or by a health care delivery organization with which the organization contracts; and/or (3) avoid the use of patient-identifiable data unless consent is obtained.

Some have suggested that IRBs should take on the responsibility of reviewing all forms of research, and perhaps many of the other uses of health information listed in the Table. For most organizations this is not currently a realistic or desirable goal. Many organizations that handle identifiable health information, even for research purposes, do not receive support or regulation from one of the 17 federal agencies that subscribe to the Common Rule and thus are not obliged to use any IRB review process. Moreover, today’s IRB is already overworked, underfunded, and undertrained for the many research reviews it is required to perform.<sup>75</sup> Adding nonresearch reviews to the IRB workload would be burdensome and probably confusing, since IRB members may tend to approach all uses of information from the research framework.<sup>74</sup> Moreover, even within the realm of research uses of information, the IRB review process was not designed to focus on protection of informational privacy, and it may be inadequate to address confidentiality concerns. Indeed, in a National Institutes of Health—sponsored study, IRB chairs reported that complaints about the lack of privacy and confidentiality protections were among the most common complaints made by research subjects.<sup>71</sup> This may, in part, be because much research involving medical records either is exempt from IRB review or is reviewed on an “expedited” basis and receives review from only one person. IRB members report that they usually rely on other organizational policies and procedures to safeguard patient privacy and confidentiality—such as an “organizational culture” of respecting patient privacy.<sup>73</sup> With additional resources and training, IRB’s will likely play an increasingly important role in privacy protection, especially for health services research.<sup>76</sup> Nevertheless, for the reasons noted and perhaps others, many organizations will find it most reasonable to assign DDB-type responsibilities to an entity that has special training and experience in dealing with issues of privacy, such as a medical records or privacy committee, or possibly to create a new committee for this purpose.

**Table: Suggested mechanisms of oversight for some common uses of identifiable health information without individual consent**

<b>Proposed Use of Information</b>	<b>Oversight Mechanism(s)</b>
Direct diagnostic or therapeutic benefit to patient whose information is at issue	Implied consent based on presenting for care
Payment for diagnostic and therapeutic care of the patient whose information is at issue	Implied consent based on submitting a bill for payment
Research covered by Common Rule	(IRB) review (mandatory)
Research not covered by Common Rule	Voluntary IRB review
Quality assurance/quality improvement projects	DDB review
Public health reporting	Legal standards
Public health research—Common Rule	IRB review
Public health research—not under Common Rule	IRB or DDB review
Marketing	DDB review
Disease management programs	DDB review
Accreditation	DDB review
Fraud detection and deterrence	Legal standards and DDB review
Fraud prosecution	Legal standards and DDB review

## Appendix 2

### *Members of the Oversight Body for the Ethical Force Program, 1999-2000*

*(Organizational affiliation listed for identification purposes)*

**Linda Emanuel, MD, PhD**

**Program Founder; Chair, 1997-2000**

American Medical Association

**Myrl Weinberg**

**Chair, 2000-2002**

National Health Council

**Robert Alpert**

United Auto Workers

**Laurie Badzek, RN, MS, JD, LLM (Alternate)**

American Nurses Association

**Michele Dennis, RN**

American Federation of State, County, and Municipal  
Employees Union

**John Eisenberg, MD**

Agency for Health Care Research and Quality

**Ezekiel Emanuel, MD, PhD**

National Institutes of Health

**Mary Jane England, MD**

Washington Business Group on Health

**Arnold Epstein, MD**

Harvard School of Public Health

**David Fleming, MD**

Center for Clinical Bioethics, Georgetown University

**Larry Gage**

National Association of Public Hospitals  
and Health Systems

**George Isham, MD**

HealthPartners

**Allan Korn, MD**

National Blue Cross Blue Shield Association

**Catherine Kunkle**

National Business Coalition on Health

**John Ludden, MD**

Harvard Medical School

**Beverly Malone, PhD, RN**

American Nurses Association

**Karen Milgate**

American Hospital Association

**Thomas Reardon, MD**

American Medical Association

**Frank Riddick, MD**

Alton Ochsner Medical Foundation

**James Sabin, MD**

Harvard Pilgrim Health Care

**Neil Schlackman, MD**

Aetna-US Healthcare

**Paul Schyve, MD**

Joint Commission on Accreditation of Healthcare  
Organizations

**Linda Shelton**

National Committee on Quality Assurance

**Drew Smith, JD**

American Association of Retired Persons

**David Tennenbaum (Alternate)**

National Blue Cross and Blue Shield Association

*Members of the Expert Advisory Panel on  
Privacy and Confidentiality*

*(Organizational affiliation listed for identification purposes)*

**Frank Riddick, MD, Chair**

Alton Ochsner Medical Foundation

**Linda L. Emanuel, MD, PhD**

American Medical Association

**Ellen Clayton, MD, JD**

Vanderbilt University

**Paul Clayton, PhD**

InterMountain Health Care

**Steve Coughlin, PhD, MPH**

Centers for Disease Control and Prevention

**George Duncan, PhD**

Carnegie Mellon University

**Bob Gellman, JD**

Privacy and Information Policy Consultant

**Denise Nagel, MD**

National Coalition for Patient Rights

**Paul Schyve, MD**

Joint Commission for the Accreditation of Health Care  
Organizations

**Linda Shelton**

National Committee for Quality Assurance

*Ethical Force Program Staff*

**Matthew K. Wynia, MD, MPH**

Ethical Force Program, Executive Director  
(Primary Report Author)

**Deborah Cummins, PhD**

Ethical Force Program, Associate Director

**Benjamin Kim**

Institute for Ethics intern

**Sheri Alpert, PhD, MPA**

Consultant to the Ethical Force Program on Privacy Issues

## References

1. Emanuel L. Professional standards in health care: calling all parties to account. *Health Affairs*. 1997;16:52-54.
2. Wynia M. Performance measures for ethics quality. *Effective Clin Pract*. 1999;2:294-299.
3. Goldman J. Protecting privacy to improve health care. *Health Affairs*. 1998;17:47-60.
4. Etzioni A. *The Limits of Privacy*. New York, NY: Basic Books; 1999:280.
5. Gostin L. Health services research: public benefits, personal privacy, and proprietary interests. *Ann Intern Med*. 1998;129:833-835.
6. Gostin L. Health information privacy. *Cornell Law Rev*. 1995;80:101-184.
7. Howell A. Experts address concerns over plans invading medical confidentiality of members. *BNA Healthcare Daily Rep*. 1998; 6(37)0.
8. *Health Privacy and Confidentiality Recommendations*. Washington, DC: National Committee on Vital and Health Statistics; June 25, 1997.
9. Marwick C. Medical records privacy: a patient rights issue. *JAMA*. 1996;276:1861-1862.
10. Westin A. 1998 Harris-Westin Survey on Privacy and the Elements of Self-Regulation. In: *Proceeding of the Department of Commerce Privacy Conference*. June 23, 1998; Department of Commerce, Washington, DC.
11. Harris-Equifax Consumer Privacy Survey, 20-29 July, 1996. Harris-Equifax, Inc; 1996.
12. Westin A. *Privacy and Freedom*. New York: Atheneum; 1967.
13. Regan P. *Legislating Privacy*. Chapel Hill, NC: University of North Carolina Press; 1995.
14. Alpert S. Privacy and the analysis of stored tissues. In: *Research Involving Human Biological Materials: Ethical Issues and Policy Guidance*, Vol. II, Comissioned Papers. National Bioethics Advisory Commission, Wash. DC 1997.
15. Chapman A. Devloping health information systems consistent with human rights criteria. In: *Health care and information ethics: protecting fundamental human rights*. Chapman A, ed. Kansas City, MO: Sheed & Ward; 1997.
16. *Ethical Issues & Patient Rights: Across the Continuum of Care*. Oakbrook Terrace, Ill: Joint Commission on Accreditation of Healthcare Organizations; 1998 156.
17. Doyal L. Human need and the right of patients to privacy. *J Contemp Health Law Pol*. 1997;14:1-21.
18. Starr P. Health and the right to privacy. *Am J Law Med*. 1999;25:193-201.
19. *Model Code for the Protection of Personal Information*. Etobicoke, Ontario: National Standards Association of Canada; 1996.
20. Hodge J, Gostin L, Jacobson P. Legal issues concerning electronic health information: privacy, quality, and liability. *JAMA*. 1999;282:1466-1471.
21. Duncan G, Jabine T, Wolf VD. *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics*. National Academy Press, Washington, DC: Committee on National Statistics, Commission on Behavioral and Social Sciences and Education, National Research Council and the Social Science Research Council; 1993.
22. Monane M, Mathias D, Nagle B, Kelly M. Improving prescribing patterns for the elderly through an online drug utilization review intervention: a system linking the physician, pharmacist, and computer. *JAMA*. 1998;280:1249-1252.
23. Sweeney L. Weaving technology and policy together to maintain confidentiality. *J Law Med Ethics*. 1997;25:98-110.
24. Armstrong M, Rushton G, Zimmerman D. Geographically masking health data to preserve confidentiality. *Stat Med*. 1999;18:497-525.
25. Ohrn A, Ohno-Machado L. Using Boolean reasoning to anonymize databases. *Artif Intell Med*. 1999;15:235-254.
26. Finkelstein K. The computer cure. *New Republic*. 1998;219:28-33.
27. Westin A. Louis Harris Associates. *Health Care Information Privacy: A Survey of the Public and Leaders*. Conducted for Equifax, Inc. (study No. 934009); 1993.
28. Americans worry about the privacy of their computerized medical records; health plans, drug companies and government health programs are least trusted. *BW Healthwire via Newsedge Corp*. Oakland, Calif; 1999.
29. Melton L. Privacy and medical records research. *N Engl J Med*. 1998;338:1076-1078.
30. Coughlin S. *Ethics in Epidemiology and Public Health Practice: Collected Works*. Columbus, Ga: Quill Publications; 1997:232.

31. Etzioni A. Medical records: enhancing privacy, preserving the common good. *Hastings Cent Rep.* 1999;29:14-23.
32. Robert E. Nolan Company, Inc. *Cost and Impact Analysis: Common Components of Confidentiality Legislation.* Chicago Ill: Blue Cross Blue Shield Association of America; 1999.
33. *Statement for the Record on the Confidentiality of Health Information.* Washington, DC: The Washington Business Group on Health; 1999.
34. Buckovich S, Rippen H, Rozen M. Driving towards guiding principles: a goal for privacy, confidentiality and security of health information. *J Am Med Inform Assoc.* 1999;6:122-133.
35. Kremer T, Gesten E. Confidentiality limits of managed care and clients' willingness to self-disclose. *Prof Psychol Res Pract.* 1998;28:553-558.
36. Goldman J, Muligan D. *Privacy and health information systems: A guide to protecting patient confidentiality.* Washington, DC: Center for Democracy and Technology; 1996.
37. Alpert S. Smart cards, smarter policy. *Hastings Cent Rep.* 1993;23:13-23.
38. Studdert D. Direct contracts, data sharing and employee risk selection: new stakes for patient privacy in tomorrow's health insurance markets. *Am J Law Med.* 1999;25:233-265.
39. Moore J. Confidentiality casualty: Patient billing printouts released in Kansas fraud case. *Modern Healthcare*; Sept. 14, 1998;3:\*\*\*
40. Michigan medical records accidentally posted on the web. *Associated Press Newswire*; February 12, 1999.
41. O'Harrow R Jr. Survey not stifled by privacy concerns. *Washington Post.* December 15, 1998:C18.
42. Brubaker B. 'Sensitive' Kaiser e-mails go astray. *Washington Post.* August 10, 2000: E1.
42. O'Harrow R. Jr. Firm tracking consumers on web for drug companies. *Washington Post.* August 15, 2000: E1.
43. Vukadinovich D, Coughlin S. State confidentiality laws and restrictions on epidemiologic research: A case study of Louisiana law and proposed solutions. *Epidemiology.* 1999; 10:91-94.
44. Pimley D. Maine experience shows potential snag as public grapples with patient privacy. *BNA's Health Law Reporter.* February 4, 1999:8.
46. McCarthy D, Shatin D, Drinkard C, Kleinman J, Gardener J. Medical records and privacy: Empirical effects of legislation. *Health Serv Res.* 1999;34:417-425.
47. *Protecting Privacy in Computerized Medical Information.* Washington, DC: Office of Technology Assessment; 1993: OTA-TCT-576.
48. Barrows R, Clayton P. Privacy, confidentiality, and electronic medical records. *J Am Med Inform Assoc.* 1996;3:139-148.
49. Campbell S, Gibby G, Collingwood S. The internet and electronic transmission of medical records. *J Clin Monit.* 1997;13:325-334.
50. Duncan G, Pearson R. Enhancing access to microdata while protecting confidentiality: Prospects for the future. *Stat Sci.* 1991;6:219-239.
51. Parsi K, Winslade W, Corcoran K. Does confidentiality have a future? The computer-based patient record and managed mental health care. *Trends Health Care Law Ethics.* 1995;10:78-82.
52. Rind D, Szolovits P, Kohane I. Confidentiality and electronic medical records. *Ann Intern Med.* 1998;128:510-511.
53. Janes G, Clutter G, Greenberg M. The health insurance portability and accountability act: New standards for health data systems. *J Reg Mgmt.* 1998:86-90.
54. *Statement on Health Data Control, Access, and Confidentiality.* American College of Epidemiology; 1999. Available at <http://acepidemiology.org/data.html>. Accessed 7/12/99.
55. ASHG statement: professional disclosure of familial genetic information. *Am J Hum Genet.* 1998;62:474-483.
56. Naser C, Alpert S. *Protecting the Privacy of Medical Records: An Ethical Analysis.* Boston, Mass: National Coalition for Patient Rights; 1999.
57. *Best Principles for Health Privacy.* Washington, DC: Health Privacy Project; 1999.
58. *Statement on Health Data Control, Access, and Confidentiality.* American College of Epidemiology; 1999. Available at <http://acepidemiology.org/data.html>. Accessed 7/12/99.
59. *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment.* National Committee for Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations; 1998.

60. *Accreditation 2000: Draft Standards for Managed Care Organizations and Managed Behavioral Healthcare Organizations*. Washington, DC: National Committee for Quality Assurance; 1999.
61. *The State of Health Privacy: An Uneven Terrain*. Washington, DC: Health Privacy Project; 1999.
62. NAIC adopts model legislation to protect consumer health information. *BNA's Health Care Daily Report*. 1998;3(179). More information available at [www.naic.org](http://www.naic.org)
63. *Reports of the Inter-Council Task Force on Privacy and Confidentiality*. Board of Trustees Reports 36-A-99 and 16-I-99. Chicago, Ill: American Medical Association; 1999.
64. *AAHP's Board of Directors Adds New Protections to Industry-Wide, Patient-Centered Initiative*. January 7, 1999. Available at [www.aahp.org](http://www.aahp.org). Accessed 10/25/00.
65. ASHG Statement: professional disclosure of familial genetic information. *Am J Hum Genet*. 1998;62:474-483.
66. *Sample Confidentiality Statements and Agreements for Organizations Using Computer-based Patient Record Systems*. Bethesda, MD, Computer-based Patient Record Institute; 1996.
67. Chilton L, Berger J, Melinkovich P, et al. American Academy of Pediatrics: Pediatric Practice Action Group and Task Force on Medical Informatics. Privacy protection and health information: patient rights and pediatrician responsibilities. *Pediatrics*. 1999;104:973-977.
68. Bluml B, Crooks G. Designing solutions for securing patient privacy: meeting the demands of health care in the 21st century. *J Am Pharm Assoc (Wash)*. 1999;39:402-407.
69. *Information for Health: An Information Strategy for the Modern NHS 1998-2005*. London, England: British National Health Service; 1998.
70. O'Brien D, Yasnoff W. Privacy, confidentiality and security in information systems of state health agencies. *Am J Prev Med*. 1999;16:351-358.
71. *Protecting the Confidentiality of Patient Information in a Rapidly Changing Health Care System: Summary of a National Conference*. Washington, DC: Health Systems Research, Inc; 1998.
72. Chamberlayne R, Green B, Barer M, Hertzman C, Lawrence W, Sheps S. Creating a population-based linked health database: a new resource for health services research. *Can J Public Health*. 1998;89:270-273.
73. *Medical Records Privacy: Access Needed for Health Services Research, but Oversight of Privacy Protections is Limited*. Washington, DC: General Accounting Office; 1999.
74. Grob G. *Institutional Review Boards: A Time for Reform*. Statement of George Grob, Deputy Inspector General for Evaluation and Inspections. Washington, DC: OIG/DHHS; 1998.
75. Office of the Inspector General Report. *Institutional review boards: A time for reform*. OEI-01-97-00193, June 1998
76. *Protecting Data Privacy in Health Services Research. Committee on the Role of Institutional Review Boards in Health Services Research Privacy Protection. Division of Health Care Services*. Institute of Medicine. National Academy Press. Washington, DC; 2000

