

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).