



Michael D. Maves, MD, MBA, Executive Vice President, CEO

February 5, 2007

Department of Health and Human Services
Room 434 E
200 Independence Avenue, SW
Washington, DC 20201
Attn: Personalized Health Care RFI

The American Medical Association (AMA) is pleased to offer comments on the Request for Information (RFI): “Improving Health and Accelerating Personalized Health Care Through Health Information Technology and Genomic Information in Population- and Community-based Health Care Delivery Systems.”

The RFI requests input from the public and private sectors on plans for developing and using resources involving health information technology (HIT) and genetic and molecular medicine, with specific reference to incorporating these capacities into evidence-based clinical practice, health outcomes evaluations, and research.

The AMA strongly supports measures to improve the effectiveness and safety of medical practice and believes that maximizing opportunities to predict disease risk early and analyzing the effectiveness of particular treatments at the population-based level are important and laudable goals. The ethical use of genomics and other advanced diagnostics, along with standardized informatics tools, to develop individual risk assessments and personal health plans may hold promise for preventing disease development. In addition, the AMA is opposed to unduly restrictive barriers to patient records that would impede or prevent access to data needed for medical or public health research or quality improvement or accreditation activities.

The AMA strongly cautions against the premature use of HIT as a means of transferring, storing and analyzing patients’ genetic information. While there have been impressive advances in the development of HIT from both a technical and policy perspective, much work remains to be done before HIT systems can be demonstrated to safeguard patients’ most sensitive health information reliably and securely. The AMA believes it is essential that issues of patient confidentiality and security of genetic data are adequately addressed prior to the electronic exchange of this information.

As noted in a GAO Report issued January, 2007, entitled “Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy,” as the use of electronic health information exchange increases, so does the need to protect personal health information from inappropriate disclosure. The capacity of health information exchange organizations to store and manage a large amount of electronic health information increases the risk that a breach in security could expose the personal health information of numerous individuals.

According to results of a study conducted for American Association of Retired Persons (AARP) in February 2006, Americans are concerned about the risks introduced by the use of electronic health information systems but also support the creation of a nationwide health information network. (AARP Public Policy Institute; Goldman, Janlori; Stewart, Emily; and Tossell, Beth, Health Privacy Project, *The Health Insurance Portability and Accountability Act Privacy Rule and Patient Access to Medical Records*, 2006-03 Washington, DC: February 2006). A 2005 Harris survey also showed that 70 percent of Americans are concerned that an electronic medical record system could lead to sensitive medical information being exposed because of weak security, and 69 percent are concerned that such a system would lead to more personal health information being shared without patients’ knowledge. While information technology can provide the means to protect the privacy of electronically stored and exchanged health information, the increased risk of inappropriate access and disclosure raises the level of importance for implementation of adequate privacy protections and security mechanisms in health information exchange systems.

A poll conducted for the California Health Care Foundation in January, 1999 tracked individuals’ attitudes and behaviors concerning medical privacy. One in five U.S. adults believes that a health care provider, insurance plan, government agency, or employer has improperly disclosed some of their personal medical information, with half of these respondents reporting that it had resulted in personal embarrassment or harm. One in six U.S. adults says they have done something out of the ordinary to keep personal medical information confidential. Patients may see multiple health care providers to avoid a consolidated record, pay out of pocket for reimbursable expenses to avoid filing a claim, ask a physician to withhold information regarding an embarrassing or sensitive condition from a medical record, lie, or avoid seeking health care altogether.

Privacy concerns are heightened in the context of genetic information because of the profound consequences that unauthorized disclosure or improper use poses not only for the patient, but for the family members of that patient. Genetic information can form the basis for discrimination against a patient in a variety of ways. Examples include serving as the basis for discrimination in employment decisions; preventing a patient from receiving credit, a mortgage or life insurance coverage; serving as the basis for denial of insurance coverage; and the potential for social stigma. Moreover, because the study of genetics is still in its nascent stages, it is currently impossible to predict the future uses of genetic data that are collected now and placed in a permanent electronic record.

The January, 2007 GAO Report entitled, "Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy," concluded that while efforts are underway at the U.S. Department of Health & Human Services (HHS) to create a comprehensive national privacy and security policy, HHS is in the early stages of those efforts. The report catalogs the challenges that the increased use of health information technology poses to protecting individuals' health privacy.

Understanding and resolving legal and policy issues remain key challenges, particularly those resulting from varying state laws and policies; ensuring appropriate disclosures of the minimum amount of information needed; implementing adequate security measures on health information systems; and determining allocation of liability or creating penalties for improper disclosures. Moreover, state and federal law are silent on an issue critical to this RFI, namely the issue of ownership and access rights for secondary uses of health data.

The AMA believes that the following principles should apply in the context of protecting a patient's sensitive health information from unauthorized use or disclosure. Physicians should release a patient's genetic information only with the patient's consent or in compliance with a warrant or other order of a court of law. It is unethical for any genetic information obtained from a physician for identification purposes to subsequently be used for other purposes, such as research, unless appropriate ethical guidelines are followed and the informed consent of the individual is obtained. Requiring that the genetic sample be destroyed or returned after the analysis necessary for identification is performed affords protection against inappropriate uses. Genetic information should be kept confidential and should not be disclosed to third parties without the explicit informed consent of the tested individual.

The AMA advocates for the following general principles governing privacy and confidentiality. The fundamental values and duties that guide the safekeeping of medical information should remain constant in this era of computerization. Whether they are in computerized or paper form, it is critical that medical information be accurate, secure, and free from unauthorized access and improper use. There exists a basic right of patients to privacy of their medical information and records, and this right should be explicitly acknowledged. Patients' privacy should be honored unless waived by the patient in a meaningful way or in rare instances when strong countervailing interests in public health or safety justify invasions of patient privacy or breaches of confidentiality, and then only when such invasions or breaches are subject to stringent safeguards enforced by appropriate standards of accountability. Patients' privacy should be honored in the context of gathering and disclosing information for clinical research and quality improvement activities, and any necessary departures from the preferred practices of obtaining patients' informed consent and of de-identifying all data must be strictly controlled. Any information disclosed should be limited to that information, portion of the medical record, or abstract necessary to fulfill the immediate and specific purpose of

disclosure. Physicians should not be required to report any aspects of their patients' medical history to governmental agencies or other entities, beyond that which would be required by law. Employers and insurers should be barred from access to identifiable medical information without patient consent, lest knowledge of sensitive facts form the basis of adverse decisions against individuals.

Should HHS choose to go forward with the program envisioned in the RFI, the AMA urges HHS to do so on a trial basis, through pilot-testing programs which includes the appropriate stakeholders such as organizations who do clinical research and who routinely handle genetic information, to develop and test systems that are reliable, secure, and acceptable to patients, physicians, and other stakeholders. Pilot programs should be conducted with the informed consent of the patients, physicians, and organizations involved.

In conclusion, the AMA recognizes the importance of prospectively preventing the development of disease through the ethical use of genomics and other advanced diagnostics, along with standardized informatics tools, to develop individual risk assessments and personal health plans. The AMA is similarly optimistic about the promise that health information technology holds for improving patient care. Nonetheless, the AMA strongly cautions against the premature use of patients' genetic information in health information technology systems before adequate legal protections and remedies exist for patients whose genetic information may be lost, stolen, or misused and before adequate HIT systems are in place to reliably and securely safeguard patients' most sensitive health information. Thank you for considering our comments. Any comments or question concerning this submission can be directed to Christina Collins at christina.collins@ama-assn.org or (202) 789-4584.

Sincerely,

A handwritten signature in cursive script, appearing to read "Mike Maves".

Michael D. Maves, MD, MBA