



John Tooker, MD, MBA, FACP
Executive Vice President and
Chief Executive Officer

Phone: 215 351-2800, Fax: 215 351-2829
Email: jtooker@acponline.org

October 5, 2009

David Blumenthal, M.D., M.P.P.
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
200 Independence Ave, SW
Suite 729D
Washington, DC 20201

CC: James M. Walker, MD, FACP
Chair, Medical Informatics Subcommittee
American College of Physicians

Re: HIT Policy Committee Privacy Comments

Dear Dr. Blumenthal:

The American College of Physicians (ACP), representing over 129,000 internal medicine physicians and medical students, is pleased to note the comprehensive attention to the complex issues of privacy being paid by the HIT Policy Committee.

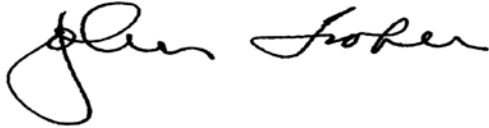
Health IT offers the opportunity to improve healthcare delivery, but only if it is coupled with comprehensive and consistent nationwide regulation and enforcement of the privacy of patient information. Many stakeholder groups are proposing complex and conflicting approaches to privacy protection. We are concerned that a rush to implement new and untested privacy protection schemes will result in unintended consequences ranging from needless impediments to care delivery to errors of omission that jeopardize patient safety.

ACP has developed a comprehensive approach to privacy that is focused on the most critical element of the equation – the relationship of the doctor and the patient. We believe that focusing on the patient alone rather than on this critical relationship will lead to inappropriate policy choices.

We appreciate the opportunity to comment as part of the Committee's deliberations on this fundamental issue, and we look forward to providing ongoing input to the HIT Policy and Standards Committees to ensure that our shared objectives for health care reform through

health IT are achievable, especially for small primary care practices. Should you have questions about these comments, please contact Thomson Kuhn at tkuhn@acponline.org or 202-261-4550.

Sincerely,

A handwritten signature in black ink, appearing to read "John Tooker". The signature is fluid and cursive, with the first name "John" written in a larger, more prominent script than the last name "Tooker".

John Tooker, MD, MBA, FACP
Executive Vice President & CEO

Attachment:

“Final ACP HIT and Privacy CPI8007.pdf”

Specific Positions of the ACP Extracted from the Paper

Position 1: ACP believes that protection of confidential data is important for the safe delivery of health care. Privacy policies should accommodate patient preference/choice so long as those preferences/choices do not negatively impact clinical care, public health, or safety.

Position 2: ACP believes that under a revised privacy rule, permitted activities not requiring consent should include well-defined socially valuable activities involving public health reporting, population health management, quality measurement, education, and certain types of clinical research. Further, ACP supports the following principles on the use of PHI and IHHI:

- A. The sale of any individually identifiable health information without the patient's permission should be expressly prohibited.
- B. Whenever possible and appropriate, de-identified, anonymized, or pseudonomized data should be used. The method used to remove identifiers should be publically disclosed.
- C. Individually identifiable information should only be supplied in cases where such information is necessary for proper performance of a specific function. For example, if the goal is to count incidence of a disease or number of patients receiving an intervention, there is no need to include individually identifiable information. Determination of the need for identifiable information should be made by appropriate publicly accountable decision making bodies (e.g., Department of Health and Human Services, regional or local Institutional Review Boards, etc.).
- D. Information that has been supplied for a particular permitted purpose should not be used for any other purpose (unanticipated use), even if permitted by regulation, without formal notification of the suppliers of the information, and, if feasible, the patient. For example, if data is collected for a single clinical study, it should not be re-used in a different study without notification as described.
- E. Use of IHHI is essential in educating current and future clinicians. There must be no restriction on the use of IHHI in educational and training activities such as grand rounds, and teaching conferences.
- F. The public must be educated about the benefits to society that result from the availability of appropriately de-identified health information.
- G. There should be tighter controls against improper re-identification of de-identified patient data.
- H. Appropriately de-identified patient data should be available for socially important activities such as population health efforts and retrospective research (with appropriate IRB approvals).
- I. We believe that patient involvement in prospective clinical research requires fully-informed and transparent consent that discloses all potential uses of patient data.

Position 3: ACP believes that whenever a health care provider discloses PHI for any purpose other than for treatment, that disclosure should be limited to the minimum data necessary for the purpose based on the judgment of the provider.

- A. While we agree conceptually that there could be benefits from application of "minimum necessary" criteria to activities involving payment and operations, current science and

technology are not up to the task. It is not possible or appropriate to disentangle elements within a clinical encounter note into relevant and non-relevant.

- B. As long as health plans require submission of complete notes from the patient record before approving payment, providers have no choice but to provide complete notes.
- C. HIT should incorporate audit trails to help detect inappropriate access to PHI.
- D. Health care providers should be required to notify patients whenever their records are lost or used for an unauthorized purpose.
- E. Health care providers should not be penalized for failure to comply with requests for PHI which, in their judgment, are inappropriate under disclosure rules after notifying the requestor that the request is being denied.
- F. Health care providers should not be held responsible for actions taken by another entity with PHI that the provider supplied to that entity in accordance with privacy regulations.

Position 4: ACP believes that privacy laws and regulations must apply to all individuals, organizations and other entities that have any contact with individually identifiable health information.

- A. Privacy protections that apply to all holders of individually identifiable health information, including services that store individually identifiable health information, should be addressed through new and comprehensive legislation.
- B. The College supports approaches that ensure that all holders of individually identifiable health information are held appropriately accountable for their actions.

Position 5: ACP believes that there must be agreement on a basic privacy model and on definitions for all terms used. There must be a single, comprehensive taxonomy for consent provisions as well as a standard structure for consent documents.

Therefore, ACP recommends that the National Committee on Vital and Health Statistics (NCVHS) convene an expert panel to address these issues.

- A. The privacy model must be unambiguous regarding which activities are permitted and which require consent.
- B. Increasingly narrowly defined consent requirements cause unacceptable burdens on people and systems, and may increase health risks and legal liability. For example, rules that allow the withholding of consent for disclosure of individual prescriptions, laboratory results, or diagnoses pose unacceptable barriers to delivery of healthcare.
- C. If consent is to operate effectively in a networked environment, the forms and content of consent artifacts must be at least as interoperable as the patient data to which they apply.

Position 6: ACP agrees that individuals should be able to access their health and medical data conveniently, reliably and affordably. Further, individuals should be able to review which entities and providers have accessed their individually identifiable health information, and when the access occurred according to the following principles:

- A. Full access to medical records and disclosure records will not be possible until EHR systems and HIEs are capable of exchanging such information in electronic form. While we support patient rights to their information, we cannot support requirements to provide the information until systems are capable of providing it in a transparent and efficient manner.

- B. Patients should have the right to request their information from every holder of information about them. Providers should be permitted a reasonable period of time to comply and to charge the patient a fee that is based on the cost of providing the information. Electronic medical records systems should be required to facilitate the provision of a patient's information in electronic formats. EHR and PHR vendors should be encouraged to ensure that their systems are interoperable.
- C. Patients should have the right to request from any provider information about disclosures of their individually identifiable information, other than disclosures made in the normal course of treatment, payment, and operations. Appropriate data would include the nature of the information, to whom it was disclosed and when it was disclosed.
- D. Electronic medical records systems should facilitate the provision information regarding all disclosures of patient data to users outside of the practice, other than disclosures made in the normal course of treatment, payment, and operations.

Position 7: Patients should have specific, defined rights to request that their individually identifiable health information not be accessed through a Health Information Exchange.

Position 8: ACP believes that patients should have complete flexibility in making disclosure choices with regard to information stored in their PHR. However, any information that originated in a PHR or that passed through a patient's control must indicate this fact as it travels through the healthcare system.

- A. It is crucial for the safety and health of the patient, as well as for protecting the liability of a provider's actions, that the source of all data in a medical record be clearly identified and maintained as the information moves from system to system because of the risk that such data could be altered and therefore not retain its accuracy and/or relevance for clinical care decisions.
- B. It is equally important that the dates and times of all creation and modification activities associated with the data be maintained with the data.
- C. If at any time patient data, which may have originated in a provider's EHR, is supplied from a PHR or other external patient-controlled systems, this fact should be assigned to the data.

Position 9: ACP believes that the nature of every agreement between entities that involves sharing of PHI should be made public.

Position 10: ACP believes that enforcement of penalties for intentional or negligent breaches of privacy should be strictly enforced and that state attorneys general should be empowered to enforce privacy rules.

- A. Recent calls for increased penalties fail to acknowledge the almost total lack of enforcement of existing penalties. See "Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight [A-04-07~05064]," (<http://www.oig.hhs.gov/oas/reports/region4/40705064.pdf>)
- B. It is critical that rules and enforcement efforts distinguish between inadvertent and intentional activities.
- C. Breach rules must not hold any parties responsible for the actions of other parties over whom they do not have direct control.

Position 11: ACP believes that new approaches to privacy measures should be tested prior to implementation.

- A. Once implemented, federal agencies and other stakeholders need to monitor the impact of new privacy measures, watch for unintended consequences, and adopt a flexible approach to implementation.

Position 12: ACP believes that use of a Voluntary Universal Unique Healthcare Identifier could provide privacy benefits and that its potential use should be studied.