ACP American College of Physicians℠
INTERNAL MEDICINE | Doctors for Adults

Health Information Technology and Privacy

Summary of Position Paper Approved by the ACP Board of Regents, July 2011

What is Health Information Technology?

Health Information Technology (HIT) is technology that enables health information to be collected, stored, and used electronically. The nature of HIT generates several kinds of important information, including individually identifiable health information (IIHI), which is any health data or record that could be correlated with a particular individual. IIHI that is transmitted by, or maintained in, electronic media or any other form or medium is considered to be protected health information (PHI).

How Does It Relate to Privacy?

As health care in the United States moves from paper to an increasingly electronic world, a new national debate over privacy of IIHI has emerged. Patients benefit when information pertinent to their care, concerns, and preferences is shared among those rendering health care services to them. However, patients need to feel confident that they can receive needed health care without the risk that their private information will be inappropriately disclosed, as such concerns might result in withholding of information and lead to potentially negative clinical consequences.

While many health policy experts and health care professionals anticipate improvements in clinical care and advances in research that could result from appropriate sharing of health information, a balance must be achieved between the need for complete, accurate, and available medical records and the requirement that all protected health information be secure and confidential to best serve the interests of the patient.

Key Findings and Recommendations from the Paper

ACP's recommendations center on the following key concerns:

- Preserving patient-clinician trust
- Addressing liability concerns among clinicians
- Defining and consistently applying an appropriate taxonomy (a set of terms that describe the range of privacy permissions) and framework
- Educating clinicians and patients about existing laws and regulations
- Protecting privacy

Specifically, ACP recommends the following:

- Privacy policies should accommodate patient preference so long as they do not negatively impact clinical care, public health, or safety.

- 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 protecting PHI and IIHI to the extent possible. Whenever a health care provider discloses PHI for a 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 revised privacy rule should maximize appropriate uses of information to achieve scientific advances without compromising ethical obligations to protect individual welfare and privacy. In addition, privacy laws and regulations must apply to all individuals, organizations, and other entities that have any contact with IIHI.
- There must be agreement on a basic privacy model and definitions, and there must be a single, comprehensive taxonomy for consent provisions and a standard structure for consent documents.
- Individuals should be able to access their health and medical data conveniently, reliably, and affordably, and should be able to review which entities and providers have accessed their IIHI.
- Patients should have specific, defined rights to request that their IIHI not be accessed through a health information exchange (HIE), a service that facilitates the exchange of patient information among physicians and other health professionals within a limited geographic area. Further, patients should have complete flexibility in making disclosure choices with regard to information stored in their personal health record (PHR), though any information that originated in a PHR or passed through a patient's control must indicate this fact as the information travels through the health care system.
- The nature of every agreement between entities that involves sharing of PHI should be made public.
- Enforcement of penalties for intentional or negligent breaches of privacy should be strictly enforced, and state attorneys general should be empowered to enforce privacy rules.
- New approaches to privacy measures should be tested before implementation.
- Use of a Voluntary Universal Unique Healthcare Identifier (an ID similar to a Social Security Number that would be assigned to a patient and used for all interactions with the healthcare system, but would not be used for any other purpose) could provide privacy benefits, and its potential use should be studied.

For More Information

This issue brief is a summary of *Health Information Technology & Privacy*. The full paper is available at http://www.acponline.org/advocacy/where_we_stand/policy/hit_privacy.pdf.