



**American Hospital  
Association**

Liberty Place, Suite 700  
325 Seventh Street, NW  
Washington, DC 20004-2802  
(202) 638-1100 Phone  
[www.aha.org](http://www.aha.org)

July 22, 2008

The Honorable John D. Dingell  
Chairman  
Committee on Energy and Commerce  
United States House of Representatives  
2328 Rayburn House Office Building  
Washington, DC 20515

The Honorable Joe Barton  
Ranking Member  
Committee on Energy and Commerce  
United States House of Representatives  
2109 Rayburn House Office Building  
Washington, DC 20515

Dear Chairman Dingell and Ranking Member Barton :

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our 37,000 individual members, the American Hospital Association (AHA) commends the bipartisan sponsors of H.R. 6357, the Protecting Records, Optimizing Treatment, and Easing Communication through Healthcare Technology Act, or PRO(TECH)T Act of 2008, on their efforts to promote the adoption of information technology (IT) by our nation's health care providers.

Seven days a week, 24 hours a day, the women and men of America's hospitals strive to improve the safety and quality of the care they provide. Research has shown that certain kinds of IT – computerized physician order entry (CPOE), computerized decision support systems and bar-coding for medication administration, to name a few – can help them in this effort. At the same time, the adoption of IT promises to improve efficiency and help control costs.

H.R. 6357 would, among other things, codify the Office of the National Coordinator for Health Information Technology (ONC), recognizing the importance of a single point of high-level coordination among several agencies. Additional provisions assuring that the new policy and standards committees will work together could pave the way for the development of appropriate standards that can achieve the bill's safety and efficiency goals.

While the AHA strongly supports the use of health IT, we also are committed to the protection of patients' health information. Historically, hospitals have worked diligently to ensure the privacy and security of personal health information, and continue to do so under the provisions of the Health Insurance Portability and Accountability Act (HIPAA). We believe that the HIPAA regulations, after considerable input from all affected parties, struck an appropriate balance between two very important goals: protecting patients' confidential health information without impeding the delivery of high-quality, timely care. We hope this critical balance is maintained as the use of health IT becomes more prominent.



While we applaud the Committee for seeking to protect the privacy and security of patients' health information, we are concerned that some of the bill's provisions will undermine this intent. Moreover, we appreciate that the Committee has tried to address some of our concerns in the Amendment in the Nature of a Substitute (AINS). But a number of problems remain.

Specifically, Section 312 (c) requires all covered entities using an electronic medical record to account for disclosures of protected health information (except for oral disclosures) made in the course of treatment, payment and health care operations. These fundamental activities had been excepted from the original, broader HIPAA requirement because the burden of collecting and maintaining this information far outweighed any potential benefit.

While electronic medical records make it feasible for audit trails to track disclosures, the sheer volume of information generated in direct care activities, payment and health care operations, and the storage capacity needed to hold the information and make it accessible and intelligible to patients, would divert already-scarce resources away from patient care.

The AINS reduces the required holding time from six to three years, which is an improvement. But tying the effective date to any upgrade of an existing electronic system or the initial use of such a system, would be a disincentive to the adoption or improvement of such systems. This would be at odds with the goal we all share: using the enormous benefits of IT to improve the quality and safety of patient care.

The second troublesome provision, Section 312(d), applies only to health care providers. It requires that a patient give written consent before the provider can use the patient's electronic medical record for "health care operations." Health care operations are clearly defined under HIPAA and, in the case of hospitals, are programs that are critical to the continual improvement of quality and safety.

For hospitals, health care operations include, but are not limited to, all internal quality assurance activities. This would include reporting of data on quality measures through the Hospital Quality Alliance (HQA) to the Hospital Compare website (Hospitalcompare.gov) maintained by CMS. It would also include participation in numerous voluntary state quality projects, such as the Keystone Project in Michigan.

Because these are voluntary programs, H.R. 6357 clearly puts these programs at risk, jeopardizing both the need for quality information and hospitals' financial viability.

Other examples of hospital health care operations are credentialing of physicians, conducting graduate medical education and training of other health professionals, and accreditation and licensing activities. Fraud and abuse compliance, medical review and legal services are also under the rubric of health care operations.

Finally, even the activities involved with de-identifying health records to make them available for epidemiological studies falls under the mantle of health care operations and would be adversely affected by this consent requirement.

The Honorable John D. Dingell and The Honorable Joe Barton

July 22, 2008

Page 3

While HIPAA protects the individual's privacy by permitting the use of only the minimum necessary amount of information for these activities, section 312(d) requires a covered provider that uses electronic medical records to obtain the consent of each patient before using for health care operations any part of the information in the patient's electronic medical record.

Even though the AINS clarifies the mechanics of consent and revocation, and delays implementation, the key problem remains: data from any patient who has not provided consent would be excluded from quality analysis, fraud and abuse analysis, sentinel event analysis, and so forth.

As a result, reports generated and conclusions drawn from data analyses for all of the quality, oversight, education and patient safety activities above would be invalid because they were performed on an incomplete sample of patient records. It is well-established that those who decline to consent are not a random sample of the population. Rather, they tend to be individuals who have heightened privacy concerns – such as may occur in individuals who have experienced a quality related incident, or individuals who have complex or sensitive health conditions. Further, the ability of patients to rescind their consent at any time could interrupt ongoing quality assurance and patient safety activities and reporting. For example, all of the follow-up information regarding a sentinel event could be lost if a patient revoked or did not provide consent; the success of infection control measures could be questionable if patients who experienced infections revoked consent, etc. For all of these reasons, the balancing of interests that has been struck by the AINS is not the correct balance with respect to the quality of care provided in the United States: the AINS protects the individual's right to control or prohibit the use of information by the hospital at the expense of the public's interest in quality care.

We urge the Committee to address these considerations as the legislative process moves forward. If enacted in its present form, the bill could adversely impact existing quality initiatives that we have worked to implement. Important data would not be provided to the public, and hospitals would be at risk of losing up to \$2 billion per year if they could not voluntarily report sufficient information to the federal government. Significant changes to the legislation need to occur.

We appreciate your attention to these concerns, and we look forward to working with the Committee as the bill moves forward to ensure that it encourages the use of health IT while also protecting patients' privacy and helping hospitals deliver timely, high quality care.

Sincerely,

Rick Pollack  
Executive Vice President