



Healthcare Information and Management Systems Society

September 2011

Recommendation to Congress

2011 HIMSS Policy Summit Ask #3:

In order to ensure that your constituent is the right person getting the right healthcare at the right time, Congress should support the development of a nationwide patient identity solution by lifting the current statutory prohibition, to allow HHS to address this issue along with other health IT policy enhancements.

Problem

One of the largest unresolved issues in the safe and secure exchange of health information is the need for a nationwide patient identity solution to allow accurate, timely, and efficient matching of patients with their healthcare data, which may be generated in multiple systems.

Congress has placed a clear priority on the nation's healthcare community for adoption of interoperable electronic health records (EHRs) and other health IT, and an increased health information exchange (HIE) capability. Additionally, the Administration has made health information technology (IT) and the ability to exchange data an essential component of the nation's healthcare transformation strategy.

However, paradoxically, Congress has simultaneously placed a huge impediment to the optimal adoption of EHRs and health information exchange. In 1996, HIPAA mandated that the Department of Health and Human Services address the need for a Unique Individual Identifier for healthcare purposes. However, the 1999 Omnibus Appropriations Actⁱ prohibited the use of federal funds to "promulgate or adopt any final standard... for a unique health identifier for an individual until legislation is enacted specifically approving the standard." That language has been carried forward in every Labor HHS Appropriations bill since.

Background

Patient-data mismatches remain a significant problem. According to industry estimates, between eight and 14 percent of medical records include erroneous information tied to an incorrect patient identity, costing hundreds of millions of dollars per year to correct and resulting in serious risk to patient safety.ⁱⁱ With the numerous benefits of EHRs and HIE also come potential opportunities for patient-data mismatches.

Since Congress enacted the restriction in 1999, health IT has made significant strides toward improving clinical care, enhancing patient outcomes, and controlling costs. Similar advances have been realized in the area of protecting the privacy and security of health information. Healthcare transformation is virtually impossible without meaningful, system-wide adoption of EHRs and health information exchange including technologically advanced national-level patient identity solutions.

HIMSS is not recommending a particular technology or solution but, rather, is encouraging Congress to reconsider its prohibition and to take steps that could lead to a nationwide approach and standards that will facilitate health information exchange, optimize patient-data matching, and enhance patient safety, privacy and security. A technologically advanced nationwide patient identity solution does not mean that every system has to use the same patient identity method but, rather, means national standards and solutions that can be used for exchanging information across systems.

An informed national-level patient identity solution would enhance, not compromise, the privacy and security of patient health information. Such a national-level patient identity solution does not mean a national identity number or card. Technological advances now allow for much more sophisticated solutions to patient identity and privacy controls, including patient consent, voluntary patient identifiers, metadata identification tagging, access credentialing, and sophisticated algorithms.

In the absence of a national-level patient identity solution, the states, HIEs, large health plans, various consortiums, and individual electronic health record vendors have had to develop their own patient identity solutions that do not necessarily work well across systems. As our nation moves forward with greater urgency toward the system-wide adoption of EHRs, this essential core functionality to ensure the accurate match of a patient with his or her information remains conspicuously absent. The multitude of different solutions and the lack of a national coordinated approach pose major challenges for our health information infrastructure. Patient safety, privacy, and security depend on getting this core element right, and soon.

An informed identity solution would provide unambiguous identification, be cost efficient, and also be tremendously effective in reducing errors in the patient matching process. As a result, such a patient identity solution is an essential building block to achieving the nationwide exchange of health information, as well as improving patient safety and reducing healthcare costs, fraud, and abuse. As the nation works to achieve the “meaningful use of certified EHR technology” and widespread information exchange, the right patient identity solution becomes an ever more critical factor for healthcare.

Solution

HIMSS recommends that Congress:

In order to ensure that your constituent is the right person getting the right healthcare at the right time, Congress should support the development of a nationwide patient identity solution by lifting the current statutory prohibition, to allow HHS to address this issue along with other health IT policy enhancements.

ⁱ The text from 1999 Omnibus Appropriations Act (not the official title) signed into law (PL 105-277); “SEC. 516. None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of Social Security Act (42 U.S.C 1320d-2(b) providing for, the assignment of, a unique health identifier for an individual (except in an individual’s capacity as an employer or health care provider), until legislation is enacted specifically approving the standard.”

ⁱⁱ Identity Crisis - An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System, Rand Corporation Study, 2008.