*Healthcare Information and Management Systems Society*

September 2012

**Recommendation to Congress**

## 2012 HIMSS Policy Summit Ask #1:
## In the interest of patient safety, privacy, and security, and in order to achieve the full potential of health information exchange, Congress should direct a study of patient data matching issues and best approaches to identify an appropriate nationwide patient data matching strategy.

### Problem

One of the largest unresolved issues in the safe and secure electronic exchange of health information is the need for a nationwide patient data matching strategy to ensure the accurate, timely, and efficient matching of patients with their healthcare data across different systems and settings of care.

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) mandated *"a Unique Individual Identifier for healthcare purposes."* However, the 1999 Omnibus Appropriations Act (PL 105-277) stated:

> *"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 the Social Security Act (42 U.S.C. 1320d-2(b)) providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard.")*

This language has been carried forward in Labor HHS Appropriations bills ever since.

Since 1999, three successive administrations have interpreted the Appropriations language to mean no study, no standards, and no criteria, i.e., not addressing the issue at all. Others believe that the language simply means no attempt to finalize a rule or solution until HHS reports to Congress on how any proposed solution will protect patient privacy and security.

With passage of the HITECH Act in 2009, Congress has placed a clear mandate on the nation's healthcare community for adoption of interoperable electronic health records (EHRs) including financial incentives for adopting EHRs and disincentives of reduced Medicare reimbursement rates for not doing so. 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; Meaningful Use Stage 2 of the Medicare and Medicaid EHR Incentive Program emphasizes this focus on health information exchange (HIE). Furthermore, data is increasingly generated outside the traditional care environment, expanding the need for sound approaches to the matching of patient data.

However, the lack of clear Congressional intent as a result of the Labor HHS Appropriations bill provision poses a huge impediment to the optimal adoption of health information exchange, endangering patient safety while raising costs. As providers increasingly communicate using HIEs, the risk of mistakenly matching data with the wrong patient exponentially increases. Compromise in data integrity may occur as information is exchanged between different entities using different hardware and software.

### Background

Patient-data mismatches remain a significant and growing problem. According to industry estimates, between eight and 14 percent of medical records include erroneous information tied to an incorrect patient

identity. The result is increased costs estimated at hundreds of millions of dollars per year to correct information. These errors can result in serious risks to patient safety. Mismatches, which already occur at a significant rate within a individual institutions and systems will significantly increase when entities communicate among each other via HIE —a Meaningful Use Stage 2 requirement – that may be using different systems, different matching algorithms, and different data dictionaries.

Since Congress enacted the restriction in 1999, health information technology 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. Nationwide healthcare transformation is virtually impossible without meaningful, system-wide adoption of EHRs and HIE, including a technologically advanced nationwide patient data matching strategy.

HIMSS does not recommend a particular technology or solution but, rather, is encouraging Congress to direct a study of the issue and the approaches to a nationwide strategy to health information exchange and optimized patient-data matching across systems, while enhancing patient safety, privacy and security. A technologically advanced nationwide patient data matching strategy does not mean that every system has to use the same patient identity method but, rather, means creating national standards and solutions that can be used for exchanging information across systems.

An informed nationwide patient data matching strategy would enhance, not compromise, the privacy and security of patient health information. Such a nationwide patient data matching strategy 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 nationwide patient data matching strategy, the states, HIEs, large health plans, various consortiums, and individual electronic health record vendors have had to develop individual patient identity solutions that do not necessarily work well across systems. As our nation moves forward with greater urgency toward system-wide health information exchange, 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 and result in millions of dollars of unnecessary costs. Patient safety, privacy, and security depend on getting this core element right, and soon.

**Solution.** HIMSS recommends that Congress:

**Direct an appropriate study of a nationwide patient data matching strategy, including: the prevalence and associated costs of patient-data mismatches nationwide, the costs of correcting these errors, the safety risks associated with NOT having a nationwide strategy, the benefits and implications of applying a nationwide strategy, the impact on privacy, security, and safety of a nationwide strategy, current and near-term technological solutions, the costs/benefits and practicality of a nationwide strategy, and best industry practices currently employed to ensure acceptably reliable patient data matching across systems while enhancing patient privacy, security, and safety, with a report back to Congress in not later than six months following enactment of this legislation.**

**The Government Accountability Office (GAO) is an appropriate entity to conduct such study.**

**References:**


1. 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
2. HIMSS White Paper, "Patient Identity Integrity" December 2009, http://www.himss.org/content/files/PrivacySecurity/PIIWhitePaper.pdf