Recommendation to Congress

2012 HIMSS Policy Summit Ask #3:
In order to realize interstate Health Information Exchange (HIE), Congress should support the harmonization of federal and state privacy laws.

Problem
The ability to exchange health information confidently and securely across healthcare systems is a fundamental requirement to transforming America’s healthcare delivery system, achieving improved quality clinical outcomes, and controlling costs. With passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act; included in the American Recovery and Reinvestment Act of 2009), Congress placed a clear priority on the 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, acting upon Congress’ clear guidance to make the financial incentive requirements increasingly stringent over time, the administration has made health information exchange (HIE) an essential component of the nation’s healthcare transformation strategy. Meaningful Use Stage 2 of the Medicare and Medicaid EHR Incentive Program focuses on HIE.

Conflicting privacy and security laws are among the most serious potential barriers to HIE adoption. Legal barriers to HIE implementation are pronounced and pervasive, from the lack of laws in some states, to many conflicting laws, legal standards and regulations in other cases. There is a lack of national guidelines for the interpretation of these laws and some existing state and federal laws are not well-adapted to HIEs. Each state has its own privacy and security laws that often conflict with other state or federal laws, causing more confusion on which law(s) applies in a given situation.

Background
Privacy - The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104-191, 110 Stat. 1936), as well as its amendments in the HITECH Act, sets a floor for national privacy laws regarding PHI. HIPAA generally permits the use and disclosure of information for treatment, payment and healthcare operations, without the patient’s written consent. However, HIPAA is superseded by state privacy laws that are more stringent. States’ privacy laws have varying levels of stringency, which makes the exchange of information between and among states challenging as the entities must know and comply with federal law, the laws of the receiving and sending states, and interpret how those laws interact.

Examples of conflicting federal and state privacy laws that serve as barriers to HIE:

1. Clinical Laboratory Improvement Amendments (CLIA) (a federal law for clinical research) restricts the providers with whom a laboratory may share health information, but states that a state law may also specify who is authorized to receive a clinical laboratory test result. Only seven states have licensing laws that allow direct access to laboratory test results by the patient. State laws have varying levels of stringency in regards to lab results:

   a) New York State requires the provider’s written consent to issue lab reports to patients except for a few standard tests results such as blood type and states that the results belong to the provider and not the patient.
   b) In New Hampshire, PHI belongs to the patient, and the laboratory may release test results only to the ordering provider without the patient’s consent.
c) Oregon permits the release of test results directly to the patient seven days after receiving the request from the patient and prior access to test results requires a written authorization from the ordering physician. After the waiting period, a patient may access the results without the provider’s concurrence.

2. Hawaii’s approximately 50 privacy laws were inconsistent with federal laws, and providers, worried about complying with the inconsistent legal patchwork, were hesitant to participate in HIE. As a result, Hawaii recently passed a bill (HB 1957) to harmonize their numerous privacy laws with federal HIPAA.

**Security** - The lack of laws, legal standards, regulations, and guidance specific to the privacy and security concerns related to HIE is also a barrier to HIE adoption and implementation. Data stewardship, the responsibility, guided by principles and practices, to ensure the knowledgeable and appropriate use of data derived from individuals’ personal health information, is inconsistent. For nationwide HIE to work, it is crucial to determine which jurisdiction is responsible for providing protections in the data exchange process or alternatively, develop rules for exchange based on a set of defined and accepted principles.

Differences in authentication requirements also greatly hinder PHI exchange. There is currently no specific legal requirement for any particular type of authentication information or processes for electronically “signing” EHRs. Additionally, all PHI created, received, maintained or transmitted by an organization is subject to the federal HIPAA Security Rule, which requires covered entities to ensure the confidentiality, integrity and availability of PHI, and identify and protect against threats to security or impermissible uses or disclosures. The HIPAA Security Rule is aimed at regulating individual healthcare organizations and is not specific to HIEs.

Finally, the lack of understanding about how all of these laws interact with each other, and to whom they apply and when, creates an enormous question regarding liability. Private and federal right of actions regarding patient privacy is extensive and can be harsh with respect to damages. A reconciliation of the differing laws and standards across a national scale being very difficult, developing rules for exchange based on a set of defined and accepted principles could lead to more innovation and implementation of HIEs and a decrease in potential liability.

**Solution.** HIMSS recommends that Congress:

**Support harmonization of federal and state privacy laws and regulations by:** (1) when considering future legislation, be aware of the roadblocks to information exchange created by the current differing laws and regulations; (2) convene hearings on the challenges and possible solutions to mitigating the divergence of federal and state privacy and security laws and regulations; and (3) direct HHS to promulgate the ONC Privacy and Security Framework to protect personal health information while eliminating barriers to interstate exchange of health information.

**Sources Referenced:**


*Organizational -* AHIMA: Electronic Signature, Attestation, and Authorship, Appendix B: Laws, Regulations, and Electronic Signature Acts

*Federal and State -* State and Federal Laws Affecting Interstate HIE (whitepaper), Policy Strategies for Advancing Interstate Health Information Exchange: A Report to the State Alliance for e-Health (Christiansen IT Law)


---

1 [http://www.ncvhs.hhs.gov/090930lt.pdf](http://www.ncvhs.hhs.gov/090930lt.pdf)
Recommendation to Congress

2012 HIMSS Policy Summit Ask #2:
In order to improve the quality of healthcare for all Americans while also reducing costs, Congress should continue its strong bipartisan support for Health Information Technology.

Problem
Health Information Technology (IT) is an essential, foundational element of any meaningful transformation of our Nation’s healthcare delivery system. While our country is engaged in a long-term debate over how to reform our healthcare system, there continues to be widespread, bipartisan support for efforts to move away from a delivery and payment system that rewards volume, toward a system that rewards efficiency and quality outcomes by enabling providers and patients to access the right information at the right time. Robust nationwide adoption of health IT, including Electronic Health Records (EHRs), Health Information Exchange (HIE) capabilities, and mobile health devices is essential to achieve effective care delivery and payment reforms; patient engagement; and enabling timely, accurate, safe, private, and secure collection and dissemination of patient information in a private and secure manner.

In these times of significantly restricted resources, Congress should continue its bipartisan leadership and support for system-wide adoption of private and secure health IT to enhance the quality of the nation’s healthcare while controlling costs.

Background
Building on the nationwide adoption of EHRs and HIEs, a health IT-enabled transformation of American healthcare will enable greater patient engagement, facilitate dramatic enhancements in research, improve the quality of clinical care, implement necessary payment reforms, and significantly enhance the nation’s population health management. Such enhancements will not only improve the quality of healthcare by ensuring readily available and accurate health information to guide clinical decision making and patient and family choices, but will improve coordination of care among settings of care and reduce medical errors, simplify business processes, and save resources.

Previous Congresses and administrations, under the leadership of both political parties, have recognized the enormous value of health IT. Recognizing the urgent need for the nation to modernize healthcare delivery with health IT as a central enabler, President George W. Bush, through a 2004 Executive Order, established the Office of the National Coordinator for Health Information Technology (ONC). Under the Department of Health and Human Services, ONC is charged with developing standards for EHRs and a nationwide interoperable health IT infrastructure.

Building on the Bush Administration’s leadership in supporting solutions that maximize the potential of health IT, President Barak Obama has continued to make health IT a national priority. Federal law encourages the adoption of EHRs and the technological infrastructure that allows for near real-time exchange of clinical information. The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act established a program to offer financial incentives and associated infrastructure
support for the adoption and meaningful use of interoperable EHRs by eligible providers and eligible hospitals.

Published research by well-respected analysts has established that national investment in a technologically advanced healthcare information infrastructure will result in significant return on investment and quality improvements for the country. A RAND Corporation study cited by the Congressional Budget Office estimated approximately $80 billion in annual healthcare savings as a result of nationwide adoption of health IT. These savings, derived from use of health IT, will result from better clinical management, elimination of redundant diagnostic tests, reduced medical errors and re-hospitalizations, increased provider productivity, enhanced continuity of care across transitions of care (hospital to home or long-term care, etc.), and reductions in fraud, waste, and abuse.

As recognized by the authors of the HITECH Act, health IT adoption presents the potential to greatly reduce healthcare delivery disparities, facilitate essential research, promote early detection and prevention, manage chronic diseases, and expand available resources and capabilities. Moreover, the benefits of health IT must be made available to currently underserved populations such as minorities, inner-cities, and rural communities. This broad application of health IT should include the ability to fully employ telemedicine, electronic prescribing, use of mobile devices, and expansion of other technology to improve the access and quality care to underserved communities where it would otherwise not be available.

Health IT has already fully demonstrated its potential to improve and simplify healthcare and achieve financial and administrative priorities such as accurate and efficient billing, payment reform, coordination of benefits, and elimination of fraud and abuse. Fundamentally, health IT improves efficiency by eliminating paperwork for providers and patients, expanding access to care, and building a healthier future for the nation.

Health IT not only has the potential to control and reduce healthcare costs but also to facilitate patient engagement in their own health and improve the quality of care for individual patients and the nation. Electronic health records improve patient care by giving the provider accurate and complete information about a patient's health, providing evidence-based clinical decision making tools, facilitating integration of the patient's healthcare delivery team, and enabling coordination of care across multiple healthcare settings.

**Solution.** HIMSS recommends that Congress:

In order to improve the quality of healthcare for all Americans while also controlling costs, Congress should continue its strong bipartisan support for Health Information Technology.

---

1 Executive Order 1335: “Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information and Technology Coordinator,” authorized by President George Bush in 2004.
2 "Evidence of the Costs and Benefits of Health Information Technology". Congressional Budget Office, 2008.
3 "The Health Information Technology for Economic and Clinical Health (HITECH) Act". Signed into law by President Obama in 2009.
4 "Improving Patient Care and the Nation's Healthcare System," Office of the National Coordinator for Health Information Technology.
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:***