

INGENIX®

Security is not Privacy

Why Current HIT Provisions May Fail

This article was prepared for general information purposes only to permit you to learn more about Ingenix and its services. Your results may vary. It is not intended as a basis for decisions in specific situations, and is not an offer or guarantee.

The information in this document is subject to change without notice.

This documentation contains proprietary information, which is protected by U.S. and international copyright. All rights are reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, without the express written permission of Ingenix, Inc. Copyright 2010 Ingenix, Inc.



Abstract

The American Recovery and Reconstruction Act (ARRA), signed into law on February 17, 2009, contains substantial funding for Health Information Technology (HIT). In particular, the ARRA generously funds efforts to make electronic health records (EHRs) a reality. Subtitle D of ARRA modifies the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations, giving individuals much greater control over how and by whom their personal medical information can be used.

While the HIT provisions of the ARRA are a landmark achievement, the Act contains a critical oversight: It does not specifically allocate funds for technologies and solutions to implement HIPAA privacy. A close analysis of the privacy issue shows that, unless a simple and effective technical solution to individual privacy is available, current HIT provisions may fail.

What is Privacy?

Privacy within health care is individual ownership and control over personal health information.

The HIPAA, enacted by Congress in 1996, set a new standard for privacy by establishing that the individual—not the payer or provider—owns health care information. In addition, it states that the individual has the power to control who can view personal health care information and decide how that information can be used.

Individuals exercising their privacy rights interact with their health care information as though they were censors releasing documents under the Freedom of Information Act. They have the power to redact any section of a given document containing information that goes beyond what they feel is “necessary and sufficient” for the requestor’s purposes.

Security vs. Privacy?

Too often, the definition of security, particularly “systems” security, and the privacy of information are unfortunately interchanged.

Security is *not* the same as privacy. Traditional HIT systems security includes:

- Secure databases against intrusion from outside, or unauthorized access
- Secure transmission of information between two or more systems

Current HIT technology is a response to the “old world” requirement that an individual’s health care information be viewed as a corporate asset, rather than something that is owned and controlled by the individual. When considered in the context of the ARRA-improved HIPAA regulations, today’s security technology is insufficient to support future privacy requirements to protect individuals.

Background on HIPAA

The HIPAA legislation consists of two parts, or titles.

- Title I of HIPAA protects the health insurance coverage of workers and their families when the policy owner changes or loses his or her job
- Title II of HIPAA contains a set of Administrative Simplification (AS) provisions designed to protect the privacy of individual health information, especially as it relates to electronic data interchange (EDI)

HIPAA to Date

Title II of HIPAA was meant to simplify and encourage widespread adoption of health care EDI. Unfortunately, health care EDI systems have not become nearly as commonplace as anticipated in 1996. To date, the number of HIPAA-covered entities that have made the transition from paper to EHR systems remains relatively small. In fact, according to a 2008 survey conducted by the Harvard Medical School, only 10 percent of hospitals indicated that they had implemented EHR systems.¹

Physician offices are no further along: Only 17 percent of all physician offices have moved to EHRs.² The main barriers to widespread adoption of electronic health systems include expense and disruption during implementation.

For physicians, especially those with established paper-based practices, the cost and labor of converting to an EHR system outweighs its benefit. Hospitals, depending on their size, might spend between \$6 and \$100 million to make the paper-to-electronic transition. The \$19 billion allocated for HIT in the ARRA not only helps alleviate some of this financial burden, it mandates a transition to EHRs across the health care spectrum. Long-term, it is believed that as more and more health care information is created, electronic health information exchanges (HIEs) will evolve to facilitate the information transfer and interoperability of the health care system.

Improved Privacy Provisions of the Stimulus Bill

Part I of ARRA Subtitle D—*Improved Privacy and Security Provisions*—strengthens the privacy provisions contained in Title II of the 1996 HIPAA regulations. The main features of Subtitle D are summarized:

Extended coverage. HIPAA-covered entities—such as payers, providers, and hospitals, as well as business associates, must adhere to the outlined and improved privacy provisions.

Breach notification. HIPAA-covered entities and their business associates must notify each individual whose health information is reasonably believed to have been inappropriately accessed, acquired, or disclosed.

Use and transfer restrictions. Individuals must expressly authorize the transfer or use of personal health information to other individuals or third parties.

Audit provisions. The federal Department of Health and Human Services (HHS) or other government agencies will conduct periodic audits to ensure that covered entities and their business associates are complying with the law. Individuals may request an accounting of how their health information is being used.

Improved enforcement. Civil monetary penalties and mandatory media notification will apply to covered entities where stated privacy provisions are compromised.

How the Privacy provisions affect the HIT initiatives

The improved privacy provisions contained in the ARRA clearly intend to put individuals in control of their respective health information.

Subtitle D's privacy provisions, however, introduce a new level of business risk into the equation for physicians, hospitals, payers, and other covered entities and their business associates. Before they venture into HIT initiatives such as EHRs, HIEs, and regional health information organizations (RHIOs), covered entities must first create and implement privacy policies and technologies that meet the requirements of the law.

Presently, simple and effective privacy solutions do not exist. For example, there is currently no way for individuals to request an accounting of how all their health care information is being used. Further, individuals cannot easily redact portions of their personal health record, protecting certain information from being used by unauthorized sources.

¹ DesRoches CM, et al "Electronic health records in ambulatory care—a national survey of physicians" *N Engl J Med* 2008; 359: 50-60 Published online June 18, 2008.

² Bakhtiari, Elyas, "Physicians Making Progress on EHR Adoption" *HealthLeaders Media*, published online January 14, 2010.

The penalties defined in Part I, Subtitle D of the ARRA are very clear, and they are much stronger than those in Title II of the original HIPAA legislation (1996). The antiquated store-information-in-a-vault and transport-it-by-armored-car style security offered by current health care IT solutions does not offer the adequate level of privacy protection required, especially in a virtual environment in which records are exchanged electronically.

As a result, payers, physicians, hospitals, clinics, and other health care entities will be wary of moving forward with EHRs, HIEs, comparative effectiveness research (CER), and other ARRA HIT initiatives until they are sure their activity will not trigger those privacy penalties. More specifically, until those key entities can first ensure they can operate freely, in an environment where privacy issues such as audit and inspection are adequately handled, health care entities of all kinds are not only likely to avoid participation, they may actually seek to directly restrict the progress of ARRA HIT initiatives as an unnecessary market risk.

Why the HIT Stimulus provisions may currently be inadequate to be effective

The need for privacy technology remains an “invisible” issue to most of the HIT world, and perhaps to those regulators attempting to foster HIT evolution. Privacy technology is as key a piece of 21st century health care infrastructure as an “intelligent electrical grid” technology is to energy conservation.

More specifically, the negative consequences brought by penalties associated with HIPAA breaches far outweigh the perceived benefits of EHRs and HIEs by hospitals, physicians, and business associates. Without government funding to act as a catalyst for EHR and HIE adoption, covered entities lack a business case to initiate a transition. But funding is only part of the issue; adequate controls and oversight are also significant roadblocks.

Unfortunately, funding for this critical piece of the puzzle is missing from the current ARRA HIT package. The general breakdown of ARRA HIT funding includes the following:

Program	ARRA HIT Objective	Funding
EHR Incentives	Medicare/Medicaid	17B
EHR Incentives	HHS Discretionary Funds	1.7B
HIEs/RHIOs	Grants to support regional or sub-national efforts towards health information exchange	\$300M
Prevention and Wellness	Evidence-based clinical community-based prevention and wellness strategies, infection reduction strategies, childhood immunization programs	\$1.1B
Comparative Effectiveness	Research into comparative effectiveness of health products and treatments	\$1B
HIT Infrastructure	Grants relating to HIEs, Community Health Centers, telemedicine, distance learning, and other HIT-related efforts	\$5B
HIPAA Privacy	New solutions and services to help organizations comply with new HIPAA requirements.	\$0

What does a privacy infrastructure look like?

The key features of a privacy technology infrastructure should:

- Include a “design pattern,” or paradigm, that treats data as though it were a private document, one that can be redacted and whose distribution can be controlled by its individual owner
- Allow individuals to interact with a single aggregated “view” of information, regardless if that information is spread across multiple databases and information systems
- Ensure that an individual’s privacy intent is respected even as that information travels through a local, regional, or national HIE network
- Support auditing, tracking, and notification of when, why, for how long and which individuals see what types of health care information
- Produce accurate extracts of an individual’s entire health record as well as a record of that information’s use
- Eliminate the overhead required to encrypt information before it travels over a network, if the network “pipe” itself is secure

Privacy and our vision for 21st century health care

If privacy is left unfunded, the vendors and organizations who must deliver EHRs, HIEs, and other essential pieces of our health care future will be forced to create project-specific privacy solutions. Such an approach will likely force unnecessary and redundant expenses, as well as the risk of siloed systems that do not interoperate. The vision of an integrated health information highway is at risk, perhaps even impossible.

Consider a world where, after spending \$20 billion on HIT, individuals must log into five separate systems to manage their personal health information. Furthermore, imagine a world in which the collection and transfer of health care information requires time consuming and unreliable manual intervention and inadequate tracking and audit controls.

For 21st century health care to become a reality, every American must view health care Web portals and other health systems as “trusted authorities.” Health care information transactions must circulate around the system with the same privacy, speed, and trust that financial transactions do today.

While the provisions of the HIT Stimulus package within the ARRA are a good catalyst for focusing interest on HIT/HIE/EHR evolution, they are currently inadequate. Increased focus must be made by respective legislative and regulatory bodies to dedicate the necessary funding to develop trusted HIE authorities, and to manage the more intricate privacy and interoperability of electronically based health information systems.

Once the foundation of individual privacy has been secured, HIE can fulfill its promise of effective, efficient transactions that help to improve the quality of health care by delivering critical information to the people that need it, when they need it.

INGENIX®

About the Company

More than 1,200 payers now look to Ingenix for solutions to their complex business challenges. By integrating a diverse suite of products and services, Ingenix helps its clients increase revenue, manage medical costs, and simplify complex administrative and financial processes with powerful data, software, consulting, and outsourcing solutions. Consistent capital investment, stability of resources, and continual innovation make Ingenix one of the largest and fastest-growing U.S. health care information companies.

About the Authors

Adindu Uzoma, Senior Fellow and Chief Scientist

As Chief Scientist, Mr. Uzoma directs the Ingenix Advanced Technology Innovations Lab where he conducts research and development work on Data Privacy & Security, Privacy-Preserving Data Mining, Hippocratic Security, Hippocratic Databases, as well as Privacy-Preserving Health Information Exchange & Sentinel Networks. Mr. Uzoma is the author of the *Virtual Hippocratic Database (VHD)*, an innovative, database-agnostic privacy enforcement technology that allow users within and across enterprises to virtually aggregate, transform, and publish HIPPA/ARRA compliant, purpose-specific virtual data extracts from remote databases on the fly.

James Krouse, Senior Director, Marketing Planning

Mr. Krouse is an established thought leader in government technology contracting and is widely interviewed and published across the industry and in the media. His extensive career in government services began as a policy analyst; he eventually became the Washington Director and Federal Liaison for the National Association of State Auditors, Comptrollers and Treasurers (NASACT), leading national Government efforts in research and representation of government financial policy, securities rules, and associated IT developments. Mr. Krouse is a certified Government Financial Manager and eCommerce Technician, and has testified before Congress on cross-jurisdictional IT applications, government financial rules, and the Federal Lines of Business (LoB) initiative.

Ingenix | Information is the lifeblood of health care | www.ingenix.com

From North America, call 800.765.6034 • ingenuity@ingenix.com

For a list of Ingenix global office locations, please refer to our website www.ingenix.com

Corporate Headquarters | 12125 Technology Drive, Eden Prairie, MN 55344

Ingenix and the Ingenix logo are registered trademarks of Ingenix. All other brand or product names are trademarks or registered marks of their respective owners. Because we are continuously improving our products and services, Ingenix reserves the right to change specifications without prior notice. Ingenix is an equal opportunity employer.

10-24644 05/10 Original © 2010 Ingenix. All Rights Reserved