



# **Striking a Balance: The Conflict and Contradiction between Patient Privacy and Information Accessibility For Achieving Improved Patient Care and Cost Efficiencies**

**Author:**

**John Tempesco**

Chief Marketing Officer  
Informatics Corporation of America



---

## **Striking a Balance: The Conflict and Contradiction between Patient Privacy and Information Accessibility For Achieving Improved Patient Care and Cost Efficiencies**

The initial driver of patient privacy in the US was HIPAA enacted in 1996. As stated in the original HHS privacy rule, a core component of HIPAA's purpose was the ability to protect patient privacy while at the same time allowing the sharing of personal health information to facilitate patient care.<sup>1</sup> As technology is finally becoming more widely used in health care, a serious divide has now emerged between advocates of patient privacy versus the essential flow of data which will improve patient care. As EHRs become more ubiquitous in physician practices, and the setting up of regional health information exchanges (HIEs) becomes more commonplace, the debate between privacy and the sharing of information for the purpose of enhancing patient care, putting the patient at the center of the health care equation, and lowering the costs of care delivery will only intensify.

## **Meaningful Use: Functionality Defined**

The goals of ARRA are ambitious and the criteria for reimbursement are demanding. Specifically, eligible physicians, including those in solo or small practices, can receive up to \$44,000 over five years under Medicare or \$63,750 over six years under Medicaid for being Meaningful Users of certified EHRs. Hospitals that become meaningful EHR users could receive up to four years of financial incentive payments under Medicare beginning in 2011, and up to six years of incentive payments under Medicaid beginning in October 2010<sup>1</sup>.

## **Unintended Consequences**

The Tiger Team created by the Office of the National Coordinator (ONC) to explore this conundrum and to form a set of guidelines has established a core set of values regarding patient privacy and trust as they relate to patient records:

- The relationship between the patient and health care provider is the foundation for trust in health information exchange.
- As key agents of trust for patients, providers are responsible for maintaining the privacy and security of their patients' records.
- We must consider patient needs and reasonable expectations. Patients should not be surprised about or harmed by collections, uses, or disclosures of their data.
- Ultimately, to be successful in the use of health information exchange to improve health care, we need to earn the trust of both consumers and physicians.<sup>3</sup>

---

## The Importance of Trust

While these values sum up the importance of trust in the relationship between physician and patient, they only lightly touch upon the role of health information exchange as the next big step in driving home many of the key goals of health reform and the successful use of health information technology. Health information exchange becomes the critical channel for delivering improved outcomes, safety and efficiency in health care, whether the environment is a hospital, an integrated delivery network, a community or a state. And while trust is essential to the patient/physician relationship, as well as the foundation of future health information exchange, trust is a qualitative variable that somehow must be embedded into policy and technology solutions in order for health care technology to effectively address the core problems of health care inefficiency, hazard and excess.

Fortunately, there is a growing awareness of the delicacy of this problem among policy makers in Washington. The Health Information Technology Policy Council (HITPC), a policy group working to develop privacy and security guidelines for HITECH, has moved ahead in developing an updated overview for Meaningful Consent, where a patient will have to decide if, when and how they will share their patient data with other physicians or other providers such that the patient will be given the best and most appropriate care. HITPC is encouraging ONC to promote this policy vigorously and it has the potential to deeply affect the adoption of many health technologies, including the expansion of health information exchanges.<sup>4</sup> Failure to adopt policies such as this will greatly inhibit, if not completely derail, many of the over-riding goals of health care reform.

New models emerging in health care delivery also present complications. Accountable Care Organizations (ACO), encouraged by health reform to engender collaboration, coordination and profit sharing among hospitals and physicians, present a unique wrinkle on the privacy vs. accessibility quandary. In addition to enhancing care by sharing resources, a key success factor to the ACO will be organizations facilitating the timely exchange of information between and among primary care, specialty care and hospitals for care coordination and transitions. It will be critical that health information exchange be both secure and “open”, that is, provide the ability for patient information to flow rapidly and freely to key parties, all the while protecting patient privacy. Seemingly, a contradiction in terms.

## Opt-In or Opt-Out

As guidelines continue to be developed, it will be important to consider the mechanisms of how patients will determine the exchange of their health information. It will also be important for policy makers to examine the balance between efficiency in how patient data is collected and distributed, and certain key aspects of patient privacy. If restrictions are too severe, the goals of ARRA and HITECH will be in jeopardy. Patients will be driven by policy to “sit on” their data which will nullify the ability of the health care system “at large” to achieve its goals of improving patient care and safety through the sharing of data, as well as reducing overall health care costs. If data is exchanged too readily without appropriate security measures, patient privacy will certainly be in jeopardy. This dichotomy is the essential conundrum.

Opt-Out most closely resembles the state of fair and controlled information exchange as it exists today. Opt-Out protects patient privacy and enables the sharing of health records unless the patient specifically opts-out. This approach would not put a crimp on the expansion of regional health information exchanges which will enable physicians and organizations in an area to have access to critical patient data in order to improve an individual's patient care as well as to identify, in the aggregate, any troublesome health trends that would require attention. The Opt-Out provision requires that the patient is given an adequate amount of time to make a decision about consent, including the situation of an urgent need of care. It also requires a clear explanation of consent choice that must be provided by the physician or hospital as well as the consequences of opting out. The receiving of necessary medical care is not conditional upon granting consent to exchange medical information. A patient has the right to revoke consent at any time. And finally, responsibility for educating the patient about consent rests with the hospital.

---

Opt-In, on the other hand, would put a halt to the sharing of patient information unless the patient “opts-in” to the system enabling the transmission of health data. This option would not only severely restrict health information exchange, and limit the ability of health information technology to improve patient care and reduce costs in regions and nationally, it would nullify many of the benefits of health information technology, particularly the multi-organizational and multi-community benefits of HIEs.

## Appropriate and Inappropriate Access

From a practical, day-to-day standpoint, how will privacy and trust be administered? John Glaser, CEO, Siemens Health Services, and former long-time and well-known CIO of Partners Health care, presented a study of the “appropriate” and “inappropriate” access of patient records at Brigham and Womens and Massachusetts General Hospitals as part of a presentation entitled, “Discovering New Frontiers for Health IT Applications” at a recent CHIME<sup>5</sup> conference. And while the study found that there was indeed inappropriate access to patient records, the majority of that access (43%) was family. The goal of the study, whose participants included Partners Health care, Harvard Pilgrim Health care, Siemens Health Services and CSC Health Services, was to identify systemic flaws surrounding access, and to increase the quality and efficiency of interactions between providers and payers to reduce the amount of inappropriate access possible in select systems.<sup>6</sup> Efforts such as this will become increasingly important as HIEs and other health IT systems progressively become a structural part of our health systems.

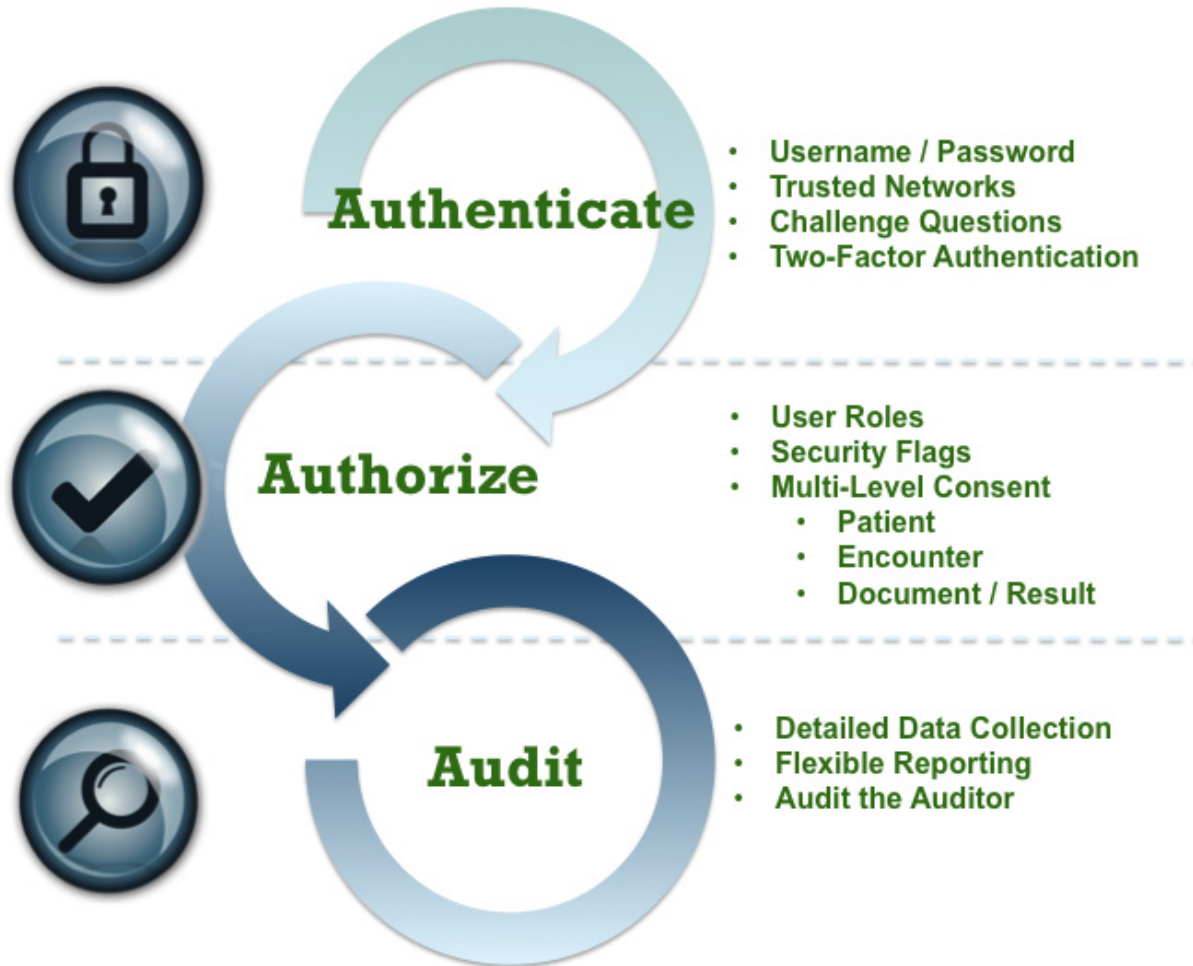
## ICA's CareAlign™ Puts Privacy and Security First

Privacy and security of patient information are ICA's highest priorities in facilitating health information exchange. The CareAlign™ solution was designed to comply with all state and federal regulations, requirements, and mandates including HIPAA and the ARRA impacts to HIPAA. ICA observes and enforces all applicable governing statutes and incorporates industry best practices and technologies to maintain customer and provider data safeguards, thus enabling trust among all participants responsible for delivering care. ICA is committed to striking the right balance between safeguarding patient data and enabling it to be shared across multiple settings in an aggregated and patient-specific way. The importance of trust between physicians and patients cannot be overstated and holds the key to a successful HIE or ACO— which is proving to be the critical channel for delivering improved outcomes, safety and efficiency in health care.

In response to heightened interest in protecting individual health information – especially in the growing multi-community Health Information Exchange (HIE) environment ICA points to the capabilities of its CareAlign™ technology solution in addressing the “Three A's” of security and privacy: authenticate – validate identity of the user seeking access to data; authorize – determine user role as the framework for allowing access; audit – trigger an examination of the system and all user activities, including data collection and audit reporting. CareAlign's™ comprehensive security supports privacy and security policies and procedures closely monitoring regulations and industry standards and working with clients to stay abreast of all requirements and updates. Our solution supports integrated authentication and authorization services for both web service and portal access. For clinical providers using the web-based portal, we use the same multi-factor authentication approach employed by the banking and credit card industries. Besides the encryption of all data in transit, data at rest are always secured in a database that has its own user authentication mechanism and are protected from access by unauthorized individuals. Once a user has been properly authenticated, the solution uses role-based authorization as the framework for managing user access to information and functional capabilities. Users are associated with a role as part of the user set-up process, and information and functional access decisions are based on those defined roles. By allowing user profiles to vary at the participant level, the technology is better able to support numerous security policies of the HIE's member institutions. Taking into account user roles,

profiles can be configured to allow or disallow access to specific categories of information and functionality. In other words, clinical users can be enabled or prevented from viewing sensitive categories of patient information such as psychiatric data, VIPs and other categories of patients.

The system also has the capability of managing patient access based on “Opt Out” and “Opt In” based on



the specific requirements of the participating organizations, the importance of which has been noted above. Patient consent levels dictate who can view data and when. Maintained at the HIE, participant, encounter and result levels, the “Opt In” and “Opt Out” functionality allows individuals to control what information is made available or can be viewed, allowing patients to opt-out at certain facilities or encounters but not others. These indicators can be maintained directly through the portal or through a feed from the participant’s source system. Patient information can also be made available to accommodate public health reporting entities based upon regulatory mandated requirements and or community or state law.

As of this writing, the ONC is still deliberating a final ruling on information exchange. While patient privacy must be attended to, clearly the critical exchange of patient information through HIEs is a central and key component to achieving the reforms of ARRA and the HITECH Act. There are numerous studies that point to health information technology as providing the necessary tools, which enable improved patient safety, and the improved efficiencies desperately needed to lower health care costs. Let us not throw out the baby with the bathwater. Let us move forward with a rational, forward-thinking approach that will ultimately get us to where we want and need to be.



**John Tempesco**  
Chief Marketing Officer, Informatics Corporation of America

## **INFORMATICS** CORPORATION OF AMERICA

### About Informatics Corporation of America (ICA)

Informatics Corporation of America's (ICA) health information exchange (HIE) solutions, originally envisioned by practicing physicians at Vanderbilt Medical Center, capture, integrate and provide comprehensive patient data from numerous and disparate installed systems. ICA adapts and deploys this pioneering technology to design and deliver comprehensive HIE solutions to hospitals, IDNs, communities and states generating cost efficiencies and improving patient care and outcomes. ICA's solutions align with physician workflow empowering caregivers to make informed decisions at the point-of-care with standards-based interoperability to help health care enterprises achieve operational efficiencies across multiple providers and settings. Visit [www.icainformatics.com](http://www.icainformatics.com), follow us on Twitter at [www.twitter.com/icainformatics](http://www.twitter.com/icainformatics), and Facebook at [www.facebook.com](http://www.facebook.com).

1 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules; 1996; <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>; accessed January 27, 2011

2 Rita K. Bowen, president, American Health Information Management Association (AHIMA) board of directors, Chicago, September 13, 2010, PRNewswire.

3 Deven McGraw, Paul Egerman, Department of Health and Human Services, HIT Policy Committee Privacy and Security Team, August 30, 2010.

4 AHIMA Foundation, Laurie A. Rinehart-Thompson, JD, RHIA, CHP; Beth M. Hjort, RHIA, CHPS; and Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS, Redefining the Health Information Management Privacy and Security Role; Online Journal: Perspectives in Health Information Management.

5 John Glaser, PhD, CEO, Siemens Health Services, Discovering New Frontiers for Health IT Applications, October 7, 2010, College of Health care Information Management Executives, CHIME10 Fall CIO Forum Track Session

6 John Glaser, PhD, CEO, Siemens Health Services, Discovering New Frontiers for Health IT Applications, October 7, 2010, College of Health care Information Management Executives, CHIME10 Fall CIO Forum Track Session



integrating care. **improving health.**