

Contact:  
(e) sales@videntity.com  
(p) +1 650.396.7717  
(w) http://videnti.com

---

**Videntity ITS:  
An Enterprise Solution for HIPAA Compliance  
in the Wake of New Health Information Technology for Economic  
and Clinical Health (HITECH) Requirements**

Videntity Identity Transaction Service (ITS), is an Internet-based application framework for building healthcare related communication applications. By providing a highly secure service, based on a patent-pending identity verification and federation mechanism, Videntity can automatically deliver and sequester information in a variety of ways; including phone, mobile phone, computer, or other devices. The service includes anti-vishing technology, which performs a two-way challenge response over the telephone enabling Videntity to secure phone based transactions and communication. Videntity is particular adept in facilitating communication with portions of the population that may seldom or never access the web.

Videntity can be used to power many types of identity communication applications. For example, the service can be used to build and power a home health monitoring application, thus reducing the need for in-home care visits. In this case it "checks-in" on individuals with chronic conditions and obtains health information on an ongoing, real-time basis. Similarly, Videntity can be used to obtain explicit patient authorization for a transaction. Videntity is a tool that was designed from the ground up to help solve many common security, privacy, and communication healthcare conundrums. Videntity also eloquently addresses many of the new security provisions spelled out in the American Recovery and Reinvestment Act (ARRA) of 2009 (a.k.a. "The Stimulus").

The Health Information Technology for Economic and Clinical Health (*HITECH*), part of the American Recovery and Reinvestment Act of 2009 (ARRA), includes provisions which make significant improvements in the privacy and security standards for health information. The provisions concerning privacy and security are primarily found in ARRA's Title XIII, Subtitle D and some parts of Subtitle A. Many of the changes, which go into effect Feb 17, 2010, can be grouped into four broad categories <sup>1</sup>:



Contact:  
(e) sales@videntity.com  
(p) +1 650.396.7717  
(w) http://videnti.com

---

- Substantive changes to HIPAA statute and privacy and security regulations
- Changes in HIPAA enforcement
- Provisions to address health information held by entities not covered by HIPAA (as either covered entities or business associates)
- Miscellaneous: Administration/Studies/Reports/Educational Initiatives

In the following sections, we briefly describe some of the new ARRA regulations and how Videntity addresss these new requirements.

**Changes in HIPAA Enforcement** - ARRA causes HIPAA to "grow teeth" and shift from guidance to enforcement. ARRA states that a covered entity's "Business Associates" are directly accountable for HIPAA. Sections 13401 and 13404 of ARRA state that business associates can be held accountable by federal and state authorities for failure to comply with any applicable provisions of the HIPAA Privacy and Security Rules <sup>2</sup>.

Under current regulations, government authorities cannot hold business associates accountable for failing to comply with their business associate agreements. Covered entities can only be held liable for the actions of their business associates in limited circumstances.

Section 13409 of ARRA clarifies that HIPAA's criminal penalties can be enforced against individuals, including (but not limited to) employees of a covered entity. This overrules a Department of Justice Office of Legal Counsel memo issued during the Bush Administration that states that only covered entities can be criminally prosecuted for violations of HIPAA. In addition, the wording of the provision may broaden the scope of activities for which criminal penalties can be attached because authorities can prosecute an individual who obtains or discloses individually identifiable health information "without authorization." <sup>3</sup>

Section 13410(a) of ARRA clarifies that HHS and state attorneys-general can pursue a civil HIPAA violation in cases where criminal penalties could attach but the Department of Justice declines to pursue the case. Section 13407 of ARRA establishes breach notification requirements for vendors of personal health records and other non-HIPAA covered entities. <sup>4</sup>



Contact:  
(e) sales@videntity.com  
(p) +1 650.396.7717  
(w) http://videnti.com

---

**Disclosures** - Currently, healthcare providers have to create a log of exchange between physicians, payers, ect. Prevoiusly, disclosures between these entities were exempt from reporting but ARRA creates a legal mandate for all entities covered by HIPAA to keep accurate audit trails of personal health information. Providers, payers, and other HIPAA covered entities are required to provide patients with a list of all of their personal health information disclosures made within the previous three years. Section 13405(a) of ARRA requires covered entities (and their business associates) to honor an individual's request to restrict disclosure of protected health information to a health plan for purposes of payment or healthcare operations if the information pertains solely to a healthcare item or service that the individual has paid for in full out-of-pocket.<sup>5</sup>

Videntity creates a framework for secure exchange between:

- Provider to Provider
- Provider to Payer
- Provider to Patient
- Provider to Patient's Guardian (spouse, parent, caregiver, etc)
- Patient to Guardian (spouse, parent, caregiver, etc)

Videntity not only provides multiple means for verifying an individual's identity, but also automates transaction authorization over the phone. This is especially important for users unaccustomed to using the web and/or mobile device technology. Each transaction requires the sender's authorization (digital signature), the subject signoff (transaction authorization) and/or the receiver's signoff (delivery signature).

Within Videntity, after a relationship is established between two or more parties, subsequent ID verification and authorization is no longer required. A social graph is created and acts as the access control list so transactions can occur with explicit consent on record. In all cases, each transaction is recorded with a complete audit trail. Files containing personal health information can also be attached to each transaction. Additionally, paper-based personal health information can be verified, authorized, sent, and delivered via Videntity using the Videntity Fax Service.



Contact:  
(e) sales@videntity.com  
(p) +1 650.396.7717  
(w) http://videnti.com

---

**Individual Right of Electronic Access** - Under the existing HIPAA Privacy Rule individuals have always had a right to access and obtain a copy of their health records ("in the form or format requested") if it is "readily producible" in such form or format, within 30 days of the request in most circumstances. The covered entity may impose a "reasonable fee" for such access or copy. Any limits on such charges are usually governed by state law.<sup>6</sup>

Under Section 13405(e) of ARRA, covered entities using electronic health records must provide individuals with an electronic copy of their record, which must be transmitted directly to an entity or person specified by the individual, as long as that directive is clear, conspicuous and specific. Any fee charged for the record cannot be greater than the entity's labor costs in responding to the request. The ARRA provisions do not change the timeframe for responding to requests for copies of records.<sup>7</sup>

Videntity streamlines communication and information exchange between the patient, their doctor, and all those involved in the patient's health portrait. As a development platform, Videntity supports many communication modes including telephone, mobile phone, Internet appliance, desktop, kiosk, fax, and web applications.

**Breach Notification** - ARRA Section 13402 requires that covered entities provide notification to individuals if their health information has been breached (business associates are required to notify covered entities of any breaches; the covered entity must then notify the individual per the requirements).

Videntity can not only be used as a framework for breach notification, but can also help prevent information breaches from occurring. By employing multiple verification modes, strong encryption, and providing a social access control list, Videntity provides a secure framework for information exchange. Regardless of the source of the breach, Videntity can be used to automatically notify an individual, or individuals, and immediate corrective action can then be taken.



Contact:  
(e) sales@videntity.com  
(p) +1 650.396.7717  
(w) <http://videntity.com>

---

**Summary** - Videntity provides systematic cost-saving measures across the enterprise. Videntity also streamlines communication and increases information flow while decreasing liability exposure related to HIPAA and ARRA.

**References** -

1-7 Center for Democracy and Technology. "Summary of Health Privacy Provisions in the 2009 Stimulus Provisions." Center for Democracy and Technology. 24 March 2009.  
<<http://cdr.org>>

