

HIPAA Security Rule Expanded

Patient Data: Account for Access-Disclosure

Compliance brief by Benjamin Wright, JD

IT Logs, Control, Meta-data, Audit Trails

Congress imposed a demanding new data security regime on all healthcare organizations. Congress more or less expects the industry (hospitals, doctors' offices, insurance companies and more) to track and account for each and every access of electronic patient information. Each time someone accesses data, the organization needs a record (a log entry) of it.

Although Congress did not express this expectation in a single, concise statement, it effectively said it in four steps. The four steps are part of the American Recovery and Reinvestment [Act](#), known as Health Information Technology for Economic and Clinical Health Act or HITECH.

To comply with HITECH's four steps, the maintenance and review of logs and audit trails will not be the only procedures "covered entities" should adopt. Employee training will be important, too. But as a practical matter application-layer logs and audit trails showing on a historical basis who accessed which information will be critical to compliance.

Data Sharing vs. Restraint of Data Sharing

Before I describe the four steps, we need to see the big picture. Like other industries, the healthcare community . . . today makes great use of information technology (computers). Although many personal health records are still on paper, computer systems are already ubiquitous in clinics, hospitals, doctors' offices and insurance companies. Email and other electronic data collection and exchange are common. Loads of patient information already get into email today, whether intentionally or otherwise.

If there is one thing that information technology excels at, it is sharing information. And the capacity for computers to promote information sharing is

good because sharing is critical to the delivery and administration of healthcare. The industry already engages in extensive sharing and collaboration by way of computer technology, and this sharing/collaboration is increasing rapidly, as it is in other industries. Lots of doctors carry BlackBerries® or iPhones®, for example.

So here's the big picture conflict: computers are about sharing data; HITECH is about data restraint and accountability. The essence of HITECH's four steps is that health entities must install lots of fine-granular controls to monitor, regulate or prevent the sharing of data. Technology is enabling easy sharing; HITECH says we need to throttle it.

HITECH's Four Steps

So what are the four steps?

First, under Section 13402 of the Act, if a healthcare "covered entity" discovers that a patient's unsecured data is accessed without authority, then the entity must notify the patient. How is this requirement to be satisfied in practice? Although the keeping and auditing of logs are not the only way, [logs](#) are very important tools.

Second, under Section 13405(c) a patient will have the right to receive from a covered entity an accounting, dating back three years, of disclosures of her protected information to anyone outside the entity. A disclosure could include the sharing of information among health care entities for treatment, payment or health operations. In other words, it could cover the exchange of treatment information from one doctor to another doctor who is not employed by the same entity as the first doctor – a very common event!

This accounting requirement only applies to electronic information, not paper. It applies to any "electronic health record," which HITECH expansively defines as electronic information about a person's health, used by health care

clinicians. (Section 13400(5)) This could include lots of day-to-day internal email in a clinic, a hospital or a doctor's office – or external email among multiple health care providers. In practical terms, the effective date for this second step varies, but could start for some data as early as 2011.

As a practical matter of compliance, this step number two will require extensive logs and [audit trails](#) showing who accessed which information and when.

Third, under Section 13405(a) a patient can request that a covered entity not disclose certain information to a "health plan." The delivery and administration of healthcare can be a very complex undertaking. Compliance with a patient request to allow X information to be disclosed but not Y information is difficult. Compliance will involve real attention and review. Again, healthcare players are going to need to implement information controls that include application-layer logs and audit trails so that this kind of patient request can be enforced and employee actions can be reviewed after the fact.

Fourth, under Section 13405(b) a covered entity that uses patient information or discloses it to another covered entity must (if the purpose is for something other than treatment) limit the information to what is necessary for the purpose. Again, this is a very subtle requirement. Effective compliance requires a lot of human attention, supervision and after-the-fact review.

Interpretation

These four steps are not separate ideas. They need to be viewed in the aggregate. In any organization, perfect compliance with the HITECH's four steps will be really hard to achieve and sustain.

Implications:

1. Healthcare organizations need to be [archiving email](#) (and other e-messages such as text) for generous periods of time. Archival allows later review of which patient information was delivered to which person (not to mention other operational functions, such as review of

who was consulted on a particular matter, at which time, and so on).

2. Any healthcare email archive application needs to support audit trails that show who accessed which particular email archive record at which time.

3. For other collaboration systems (non-email), healthcare firms will similarly need [access logs](#) and audit trails.

The concept of health-care covered entities maintaining audit logs is not new. The existing HIPAA Security Rule already requires that covered entities, "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."¹ But as written that rule does not require the implementation of logs. HITECH adds urgency to such implementation.



Benjamin Wright, strategic advisor to Messaging Architects, [experts](#) on the archival and protection of email and other data in the healthcare industry.

¹ Data access audit trails are already part of other medical privacy law. New Mexico's Electronic Medical Records [Act](#), SB 278, for instance, requires a "record locator service" (a kind of clearinghouse for health records) to maintain detailed audit logs on the access of patient information.