



Aggressive HIPAA Enforcement Is Happening

Waiting for the Shoe to Drop

Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. For the last 13 years, healthcare professionals have been waiting for “the other shoe to drop” when enforcement really started. How would HIPAA enforcement affect Personal Health Information (PHI) and Electronic Patient Data (EPD)? How would the law ensure access to needed medical information while protecting EPD?

On August 4, 2009 the Secretary of Health and Human Services (HHS) announced that, effective immediately, the Office of Civil Rights (OCR) is now the enforcement arm for HIPAA.

For those in the healthcare industry this was more than the long-awaited shoe dropping. This was an industry wake-up call to make information security a top priority by not only securing patient health information, but also ensuring it remains private.

As you recall, ARRA (American Reinvestment and Recovery Act of 2009) created much stronger HIPAA fines and penalties. While many in the industry expected increased compliance, the move to OCR was unexpected. It changed indifferent enforcement into a focused legal mandate.

What OCR Enforcement Means to You

OCR has a long and successful history of moving “social” change from the lofty heights of academic debate to the front lines of legal enforcement. It is known for developing case law around ambiguous legal descriptions, which is exactly what we are seeing as standards and case law are now defining “meaningful use” and “reasonable access.”

Within 24 hours of its official delegation of HIPAA compliance responsibility, OCR announced it settled the first of several legal cases. Many involved people in clinical roles viewing Electronic Health Records (EHR) when they

had no clinical or business reason to read the file. These lawsuits illustrate the aggressive new level of enforcement now happening in healthcare.

This is the first time the government prosecuted HIPAA PHI viewing, both criminally and civilly. In these cases, nurses, doctors, and employees were fired, suspended, and fined for reading a patient file without having a valid reason to access it. They were found guilty even though they did not share, sell, or even discuss this patient’s information.

It was the “no need to read” that made this a historic case.

The Time is Now for Healthcare Data Security Systems

For a long time, the healthcare industry has put off investing in data security systems that are now commonplace in other data sensitive industries, such as banking and government. The industry avoided spending the capital because it believed there was little need until the government began serious enforcement. This was not an unjustified belief. Before turning HIPAA compliance over to the OCR, HHS’s focus has been on prosecuting fraud and abuse of medical payments and billing.

Given these facts, hospitals and practitioners believed it was better to focus their IT budgets on clinical software. IT security (other than using a basic password) usually was a victim of the budget ax. Physician and nurse complaints let them share passwords or simply bypass them altogether, making security even more lax.

Now that ARRA and the OCR make these investments mandatory. HIT security has become a high priority.

Healthcare practitioners must purchase secure data systems to comply with the law and stay off the OCR’s radar. Systems will have to show they have proactively complied with HIPAA’s security and privacy standards to avoid a “breach” of data security.

Positives and Negatives

Practitioners will also have to launch aggressive reviews of policies, access controls, system availability, and audits to find all data sources that may contain PHI. This includes scouring even long dormant data system and storage devices.

The new environment is creating positive changes. These secure systems produce electronic health records that shift more and more patient data into standardized data sets. Say “sayonara” to the centuries-old practice of paper charting with each care provider having his or her own chart using his or her own charting data definitions. Say “hello” to the promise of shared data records that are transportable across providers. EHRs create the ability for healthcare professionals to have reliable, accurate data when and where needed. Such records allow patients to have more health “management” instead of disease treatment.

However, this poses several challenges in terms of data security, access to PHI, audit trails, and data accuracy. For example, who “owns” the medical records that may reside in many different healthcare providers’ EHR databases? Who is going to pay the cost of supporting them? How can a patient change information that they find to be incorrect or that they do not want to have in that record? How can a patient “opt out” of EHR use?

Over time, the industry will sort out these questions.

Meeting the Challenge of Historic Change

Long-term this will be one of the most historic moments in medical care. Changing an entire industry from independent islands of information to one of shared meaning, shared purpose, and shared risk will at times seem scary, challenging, or seemingly impossible.

When President Kennedy called for a national goal to send men to the moon and return them safely to the earth, the U.S. had not yet achieved a successful orbit of a man around the earth, much less the moon. When he gave that visionary speech only Alan Shepard had been able to get into space for the U.S. Up to that point, most rockets fired had close to a 100 percent failure rate.

But as he said, “We choose to go to the moon in this decade and do the other things, not because they are easy, but because they are hard, because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one which we intend to win.”

As we explore how all of the needed changes will occur in healthcare technology, let’s remember that no matter how long, steep, dangerous or difficult the roads, all journeys start with the first step.

[For more information about any of our service offerings, please contact your Dell representative or visit \[dell.com/services\]\(http://dell.com/services\).](#)