Recent Changes to HIPAA and the Impact on the Information Destruction Industry

May 5, 2009

National Association
for Information Destruction, Inc.

Background

On February 17, 2009, President Obama signed the American Recovery and Revitalization Act of 2009(ARRA) into law. Included among the many initiatives to stimulate the economy was one that encouraged the continued development and promotion of standardized, electronically-based, medical records systems. In fact, this has been a stated government goal for almost two decades. Fear over the use of electronic records back in the mid-1990 is what originally prompted the inclusion of the Privacy Rule and Security Rule in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Between 2001 and 2003 (depending upon the size of the organization), healthcare providers, ranging from major hospital chains at the large end, to doctors' offices on the small end, geared up for HIPAA compliance. What resulted was a field day for HIPAA consultants. The ramp up to HIPAA compliance was also a major driver for growth of the secure destruction industry as "Covered Entities" looked to plug any potential leakage of Protected Health Information (PHI).

In reality, the language within HIPAA that drove this increased demand for secure destruction services was rather non-specific. Within the Privacy Rule, HIPAA states that Covered Entities must take steps to prevent unauthorized access to PHI on all media. That's it. There is no specific mention of shredding or information destruction whatsoever.

Another provision of HIPAA required that Covered Entities have a contractual relationship with any third-party with whom they would expose the PHI they were responsible for protecting. These third parties are Business Associates and secure destruction companies fall under that heading. The contract had the primary purpose of binding the Business Associate to elements of the HIPAA Privacy Rule and Security Rule but also served to hold the Business Associate accountable to follow agreed upon procedures for protecting PHI. (NAID has made a HIPAA Business Associate contract available to members since 2003).

While the feeling was not universal, most felt that the secure destruction industry benefited from the new status of Business Associate. For most, it meant that the information destruction decision was being handled at a much higher level within the medical community.

As has happened with most information protection legislation (with some important exceptions), the rush for compliance was followed by a conspicuous lack of enforcement. Further, the overarching goal of creating an environment that would promote development of an electronic medical records infrastructure was on a slow boat to China.

In time Covered Entities became more lax in their compliance with HIPAA (although not necessarily more lax on information disposal) and many legislators came to think of it as impotent. Just a few years ago, Senators Kennedy (D-MA) and Leahy (D-VT) proposed an overhaul of healthcare information security that essentially scrapped HIPAA in favor

of a tougher regime. The proposal failed but indicates the level of dissatisfaction with HIPAA's effectiveness.

The drafters of ARRA recognized the opportunity to frame the issue of electronic health records as an economic stimulus issue. Legislators (and the Obama administration) also saw the opportunity to improve the information security provisions of HIPAA. The name of the law contained within the ARRA that modifies HIPAA is the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

Summary of ARRA/HITECH Modifications

Among the changes in the modified HIPAA, those that will either directly or indirectly impact the information destruction industry are related to enforcement, jurisdiction, and new requirements. Even where the changes are directly aimed at Covered Entities, for better or worse, those changes will force them to examine what they expect from their Business Associates.

The changes discussed within this analysis that to some degree impact the information destruction industry are:

- The Creation of a New Class of Covered Entities
- States' Attorneys General Now in Charge of Enforcement
- Fines are increased from $25,000 To $1,500,000
- Fines are Mandatory for Information Disclosures involving "Willful Neglect"
- The Creation of the First Health Data Breach Notification Requirement
- HIPAA Regulations are Now Extended to Business Associates
- Covered Entities are Required to Evaluate and Revise All Business Associate Contracts

The Creation of a New Class of Covered Entities

When HIPAA (1996) was created the Internet and web-based healthcare services did not exist. The ARRA creates a new type of Covered Entity of companies, mostly web-based, that collect what is called Personal Health Records (PHR). Examples of PHR are information that relates to past, present or future payment for healthcare or records that relate to the condition of an individual such as their weight or their eye glass prescription. Included as examples of organizations that handle PHR and were previously not covered by HIPAA are websites offering personalized health management, companies selling dietary supplements and even web-based services to which blood pressure cuffs, blood glucose monitors or other devices are attached to store and track information. These new Covered Entities under HIPAA are called "PHR related entities" and fall under the jurisdiction of the Federal Trade Commission (FTC). Traditional Covered Entities, organizations that provide healthcare services and/or maintain health care records continue to fall under the jurisdiction of Health and Human Services (HHS).

Why does this matter to information destruction contractors? It matters because it hypothetically creates a much greater sensitivity to information disposal by a new class of

organizations covered by HIPAA regulations. Regulations, as you will read, which are much stricter than they have been in the past.

It would be remiss not to state that organizations that provide third party services to PHR related entities (this includes secure information destruction companies) are classified as "third-party service providers" when providing such services, not "Business Associates." So, while a contract is required between the two, it remains to be seen whether or not the Business Associate contract will suffice or a "third-party service provider" contract will be required.

Stronger Enforcement

Most observers intuitively felt that the new administration would usher in a stronger data protection enforcement ethic. While only time will tell if that is true, the new HIPAA requirements certainly support that conclusion.

As described previously, "HIPAA enforcement" had come to be considered somewhat of an oxymoron. HHS openly stated that it would not take punitive action in response to complaints but rather focus on a strategy of helping violators achieve compliance.

That seems to have changed.

States' Attorneys General Now in Charge of Enforcement

The first indication that there will be more aggressive enforcement of HIPAA requirements is the fact that there is a new sheriff in town. While HHS has not been stripped of its enforcement responsibilities effective immediately every state's Attorney General has clear and explicit authority to enforce HIPAA. It is highly doubtful that the top law enforcement official in each state, once they have a full understanding of the regulation, will take as conciliatory a view of HIPAA compliance as the HHS has. Keep in mind, most data breach related fines to date, completely unrelated to HIPAA, are the result of charges filed at the state level.

Increased Fines

Another not so subtle hint that the new administration is more interested in enforcement as a compliance tool is that the fine for a HIPAA complaint are increased from $25,000 to $1,500,000 - a jump of 6,000 percent. Further, fines for such violations are mandatory where such transgressions are deemed to involve "willful neglect."

Healthcare Data Breach Notification

For all organizations afloat in the HIPAA ocean, probably the most significant modification to the regulation is the creation of the first national data breach notification provision. Currently, 44 states require organizations to notify affected individuals, legal authorities and the media in the event of a data breach related to personal information. However, only two of those states require such notification for breach of healthcare data (California and Arkansas). So this is new territory on those grounds alone. But, beyond

being national in scope and beyond the fact that it includes healthcare information, the new healthcare data breach notification provision is significantly tougher than the other state notification requirements primarily because there is no "risk to harm" threshold. In other words, unlike the state requirements, notification must be given regardless of the sensitivity of the information or the potential risk. Notification must be provided in all cases of breaches where individuals names are linked to any healthcare information.

Business Associates are also legally bound by the new requirement to inform a Covered Entity of any potential breach they cause. There is currently some confusion related to the timing of such notification. Covered Entities are being given 60 days from the time they know (or should have known) about the breach to notify the appropriate bodies. However, Business Associates are also given 60 days to notify the Covered Entity of any breach they cause. Apparently, the times run concurrently, and so hypothetically, a Business Associate could inform the Covered Entity of a breach giving them little or no time to comply with the notification requirement.

As this is being written, NAID is examining the full text of the FTC's version of the notification rule. HHS has yet to release theirs. Hopefully, these documents will clear up any confusion regarding the timing requirements of breach notification.

Nonetheless, breach notification is significant to secure destruction companies primarily because Covered Entities will likely seek remedies and/or indemnification for breaches by Business Associates that result in notification incidents. Further, should a secure destruction service be party to a breach notification incident, it is likely to be made very public and expensive. With this much at stake Covered Entities are likely to add a level of scrutiny to vendor selection, evaluating the ability of the vendor to respond and protect them from such an event. Lastly, with regard to electronic information destruction, this will hasten the trend toward use of encryption technology.

There is another level of significance to the new HIPAA Health Data Breach Notification provision that goes far beyond its current scope. Breach notification has been one of the major hold ups (along with committee jurisdiction issues) on every national data protection law that has circulated in the last 5 years. There is little doubt that the notification provisions now in HIPAA are a glimpse at what will likely emerge as a general personal/financial/healthcare breach notification provision of a future data protection bill – most likely with a strong destruction requirement.

Busy Business Associates

While breach notification may be the most universally significant modification to HIPAA contained in the ARRA, there are a couple of changes that are just as significant to Business Associates.

1) Reevaluation and Renegotiation of Business Associate Contracts

Post-ARRA HIPAA specifically requires all Covered Entities to revise all Business Associate contracts to include the new provisions, including language related to the breach notification requirements. With fear of more aggressive enforcement, higher

fines, and breach notification weighing heavy on the minds of Covered Entities, it is very likely they will also be reevaluating their choice of Business Associates. For those ready to capitalize on this increased exposure, the fact that healthcare contracts may be put into play is not bad news. (See "Getting Ready for the New HIPAA" in the upcoming June 2009 *NAIDnews*). For those who need to move in that direction, the good news is that Covered Entities will be in no hurry to renegotiate. The biggest risk to any existing contract in the near term is that a competitor who is prepared will prompt the Covered Entity to reevaluate the contract sooner rather than later. In many cases it will boil down to what vendor is ready first. (NAID Members will soon have access to a new Business Associate contract incorporating the new HIPAA required elements).

2) HIPAA now extends to Business Associates

Prior to the ARRA, vendors to Covered Entities were legally required to comply with provisions of HIPAA only to the extent that the Business Associate contract bound them. Said another way, if there was no Business Associate contract in place with the Covered Entity, HIPAA did not apply to the vendor.

Post-ARRA HIPAA changes that. Any company that provides services to a Covered Entity that involves exposure to PHI, regardless of any contract that is or is not in place, is now legally bound to the applicable provisions of HIPAA. This has caused some observers to ask why the Business Associate contract is still required (since its original purpose was to bind the Business Associate to HIPAA). But regardless of this apparent redundancy, being legally bound to the provisions of HIPAA, now with a stronger enforcement regime, substantially increased fines, and breach notification, certainly raises the compliance threshold and risks for all Business Associates.

Conclusion – Get Prepared

Most of the modifications to HIPAA, such as the increased fines, Attorney General enforcement, and Business Associate being legally bound by its provisions are already effective. The notification provisions will be effective 30 days after the issuance of the final rules from the FTC and HHS (anticipated this fall).

Privacy analysts universally predict that the modifications raise the stakes substantially for all involved and expect much more attention on compliance, contingency planning (for instance planning for a notification event) and Business Associate selection. All agree that the best strategy is to be prepared.

NAID has already retained one of the country's leading privacy attorneys to draft a new HIPAA Business Associate contract under that logic that it is far better to be prepared with a new contract from a credible source than to be caught by surprise when a competitor goes in with one. The new contract along with orientation seminars will be available to members soon. In addition, NAID will be notifying the healthcare community of the availability of the new BA contract to drive interest in contacting NAID members.

NAID will also be modifying the Compliance Toolkit to include breach notification contingency planning and promoting the Toolkit as a way for HIPAA Covered Entities to meet their compliance requirements. At the same time, NAID has already announced that it will conduct intense Compliance Toolkit Training Workshops across the country to prepare its members for the opportunity to use it.

Lastly, NAID is already at work on new insurance programs to address client's exposure to professional liability claims and notification incidents. It remains to be seen how the association's work and research in this area will turn out but it is a safe bet that HIPAA Covered Entities will be interested in their Business Associate's ability to protect them from exposures stemming from retaining their services.

The last decade has proven that the information destruction industry benefits from increased attention on data protection and increased scrutiny of performance standards.

It has happened before and it will happen again. Whenever the stakes have been raised for our industry, it has proven to be an opportunity for quality service providers to excel.
