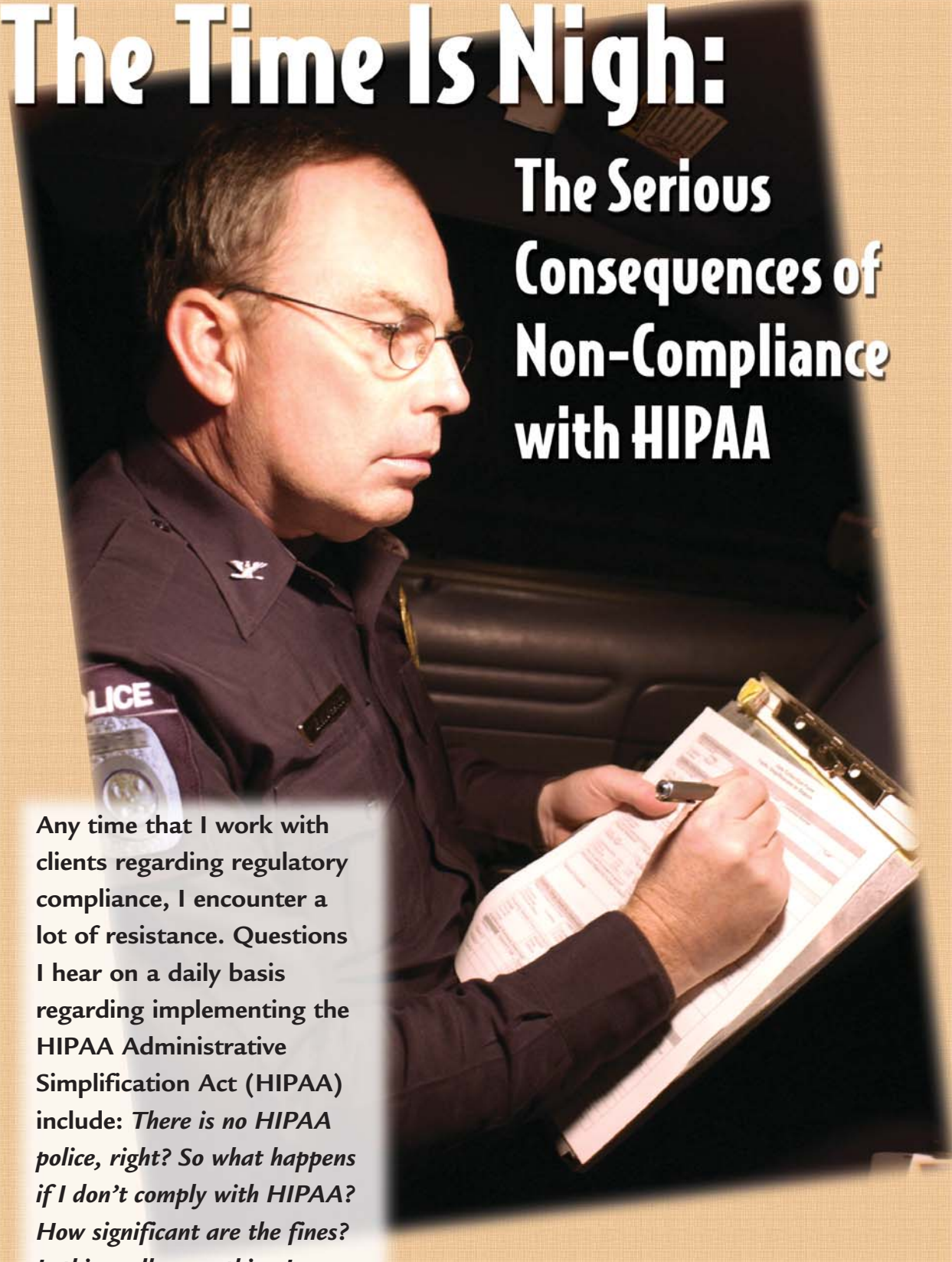


# The Time Is Nigh:

## The Serious Consequences of Non-Compliance with HIPAA



Any time that I work with clients regarding regulatory compliance, I encounter a lot of resistance. Questions I hear on a daily basis regarding implementing the HIPAA Administrative Simplification Act (HIPAA) include: *There is no HIPAA police, right? So what happens if I don't comply with HIPAA? How significant are the fines? Is this really something I should be concerned about?*

by Annette Miller, JD  
Chief Compliance Officer, HIPAAAnswers  
Eden Prairie, MN

The government has implemented several ways to enforce HIPAA. It is important to understand that the potential risks for violating HIPAA are many and may include individual complaints, government investigations, civil judgments, civil monetary penalties, criminal fines, jail sentences and loss of reputation. This article will address the enforcement mechanisms that are currently in place and the consequences of not complying with HIPAA.

## Compliance Reviews

The HIPAA regulations allow for the secretary of Health & Human Services to conduct compliance reviews to determine whether employer-sponsored health plans, providers and clearinghouses (“Covered Entities”) are in compliance with HIPAA. So what does this mean for you and your clients?

A Covered Entity is required to maintain records and submit compliance reports to the secretary upon request. In addition, the Covered Entity is required to allow the secretary access to policies, procedures or practices, books, records or other information when the secretary is conducting a compliance review or investigating a complaint. Obviously, some of this information may actually be maintained by the business associate; therefore, the business associate will need to make available these documents to the secretary as they pertain to services provided on behalf of the Covered Entity.

To date, the secretary has not implemented any formal compliance reviews. The focus to determine compliance for Covered Entities has been primarily complaint-driven. This means that when a complaint is filed against the Covered Entity, the secretary will conduct an investigation and determine compliance at that point.

Once I explain this to our clients, I often hear something like, “No one is likely to file a complaint against me. I have always taken precautions when dealing with matters we now call protected health information.”

At times like this, I always caution the client’s thinking behind these thoughts. Filing a complaint is extremely easy for an individual and it only takes one disgruntled employee to send you scrambling for those required written policies and procedures. Then the next big question becomes: Did you really follow those written policies and procedures? As we all know, there is a difference between talking the talk and walking the walk.

## Filing Complaints

Another protection put in place to allow individuals more control over their protected health information (PHI) is the ability to file a complaint against the Covered Entity for improper uses and disclosures of PHI. There are actually two complaint processes under the HIPAA regulations.

First, a complaint may be filed for non-compliance with the transactions and code sets. The Centers for Medicare/Medicaid Services (CMS) is responsible for investigating and handling these types of complaints. The steps an individual needs to take include:

- ✓ Submitting the complaint in writing on paper or electronically. The individual may use the Electronic Health Care Transactions and Code Sets Complaint Submission Form.

- ✓ The complaint must include the name of the entity subject to the complaint.

- ✓ The complaint must describe the acts or omissions to be believed in violation regarding the transaction and code set regulation.

Second, a complaint may be submitted for non-compliance with the privacy regulation. This type of complaint is submitted to the Office of Civil Rights (OCR) for investigation. The steps are similar to the other type of complaint. The complaint:

- ✓ Must be in writing and submitted on paper or electronically (using the OCR Health Information Privacy Complaint Form).

- ✓ Must include the name of the entity subject to the complaint.

- ✓ Must describe the acts or omissions to be believed in violation of the privacy regulation.

- ✓ Must be filed within 180 days of when the individual knew that the act or omission occurred.

- ✓ Must be filed at the regional OCR office overseeing the state where the alleged violation took place.

***...the potential risks for violating HIPAA include individual complaints, government investigations, civil judgments, civil monetary penalties, criminal fines, jail sentences and loss of reputation.***

Once the complaint is filed, CMS or OCR has the right to investigate activities related to the incident, including a review of the Covered Entity’s policies and procedures, business practices and the circumstances leading to the incident. The Covered Entity must permit access by the government officials to its facilities,



***If the offense is committed under false pretenses, the offender may be punished by a fine of up to \$100,000 or imprisonment for not more than five years, or both.***

books, records, accounts and other sources of information.

So what is the likelihood that a Covered Entity will have a complaint filed against it?

A review of the current number of complaints may provide some clues. For large group health plans and providers, the compliance date for the privacy regulation was April 14, 2003 — almost a year ago. In about the first three weeks of the compliance date, there were more than 70 privacy complaints filed. By June, that number had grown to 637. The most recent number, as of September (approximately five months after the compliance deadline date), is over 1,800 complaints filed. I have read that the HHS predicts that more than 24,000 complaints are likely to be filed within the first year.

Considering how easy it is to file a complaint, it is likely this will be an avenue for disgruntled employees or customers to pursue against a Covered Entity.

### **Fines and Penalties**

HIPAA has established a range of potential civil and criminal penalties for violating the law. Civil monetary penalties that may be imposed include up to \$100 for each violation, with an annual

cap of \$25,000 for all violations of an identical requirement by a single person.

A potential criminal violation will be referred to the Office of Inspector General (OIG) for further investigation, then to the Department of Justice for prosecution. A criminal violation may result in a fine of not more than \$50,000 or imprisonment for not more than one year, or both. If the offense is committed under false pretenses, the offender may be punished by a fine of up to \$100,000 or imprisonment for not more than five years, or both. It gets worse: If the offense is committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm, the offender may be punished by a fine of not more than \$250,000 or imprisonment for not more than 10 years, or both.

While it appears that in most cases the fines and penalties are assessed to the Covered Entity, business associates also need to be especially careful about being in compliance with the HIPAA regulations. In most cases, the business associate contract will include indemnification language making the business associate responsible for paying any fines or penalties assessed against the Covered Entity that result from the business associate's negligence. As for the criminal penalties, the Department of Justice has indicated that it will actively pursue business associates and individuals for criminal violations under the HIPAA regulations. They are not limiting their actions to Covered Entities.

Remember: Violations of HIPAA are potential violations of ERISA as well. Health plans are required to amend their plan documents in order to use and disclose protected health information. Under ERISA, failure to administer the plan in accordance with the plan documents is a breach of fiduciary duty. Failure to comply with the HIPAA-mandated amendments to the plans would likely be considered a breach of the fiduciary duty and a violation of ERISA.

### **Enforcement Rule**

There is an administrative process in place in the event HHS imposes a civil monetary fine on a Covered Entity. An interim enforcement rule issued in April 2003 sets forth the procedures for investigating HIPAA violations, imposing penalties and conducting hearings for appealing the penalties. The final rule is expected to be completed before September 16, 2004, when the interim rule expires.

The enforcement rule establishes the procedures for providing notice and an opportunity for a hearing to a Covered Entity after HHS makes a determination to impose a civil monetary fine. The rule provides for investigational subpoenas, witness testimony and production of other evidence for the secretary of HHS to conduct an investigation. If a penalty is proposed after an investigation, the secretary must notify the Covered Entity in writing of the intent to impose the penalty.

The Covered Entity may then request, in writing, a hearing before an administrative law judge. If a hearing is requested, each party has a right to be represented by an attorney, conduct discovery, present evidence, examine and cross-examine witnesses, present oral arguments and submit written briefs and proposed findings of fact. The administrative law judge's decision is the secretary's final decision. However, the secretary has full authority to settle the matter with the administrative law judge's consent before disposition of the matter. Either party has the right to appeal the final decision to the district court.

## State Law Claims

Regardless of how aggressively HIPAA is enforced, a larger threat for non-compliance comes from lawsuits brought by individuals under state laws. Many states recognize a statutory or common law duty of confidentiality of protected health information. A breach of this duty can lead to significant recovery of monetary damages. Therefore, HIPAA may expand the scope of a breach of confidentiality by providing a higher and more detailed standard for the proper use and disclosure of protected health information. This means employers may be required to meet the HIPAA standards under state law — even though employers are not technically covered under HIPAA.

Other state laws that Covered Entities and business associates should be aware of include: invasion of privacy, consumer protection laws for "unfair or deceptive practices," torts of fraud, defamation, publication of private facts, placing a person in a false light, misappropriation of a person's name and breach of contracts. Damages under these laws can be substantial. In many states, awards may potentially include treble (triple) damages and attorney fees.

Additionally, the publicity to a Covered Entity or business associate's business when a criminal investigation is being conducted or a state lawsuit has been filed could have serious consequences as well.

## Conclusion

How does the Covered Entity or business associate minimize its liability? First, you must take the compliance process seriously. Simply ignoring it will not make it go away. The Covered Entity or business associate needs to use reasonable efforts to try to comply.

Second, you and your clients must recognize the compliance process will take time and effort. But it is feasible to complete the necessary steps, within the set deadlines, if you find a HIPAA compli-

***As for the criminal penalties, the Department of Justice has indicated that it will actively pursue business associates and individuals for criminal violations under the HIPAA regulations.***

ance solution such as that offered by HIPAAAnswers, the firm I represent. It allows you to work through one HIPAA requirement at a time and provides you with sample policies, forms, correspondence and training guides. Regardless which firm you or your client select, a HIPAA solution can help

cut down on the time and expense of implementing HIPAA.

In addition, state laws cannot be ignored as they pose a greater threat. Don't forget to conduct a preemption analysis and include the state law requirements. Training is another key factor. Drafting policies and procedures and placing them on a bookshelf will not offer enough protection. It is important that the employees understand and follow the established policies and procedures. Finally, make sure you have a process in place to update the policies and procedures as the laws or business operations change.

Good luck. The deadline is looming but there is still time to comply if you and your clients act now. ■

***Regardless how aggressively HIPAA is enforced, a larger threat for non-compliance comes from lawsuits brought by individuals under state laws***

---

*Annette Miller has more than 15 years experience in the health insurance industry. She graduated cum laude from William Mitchell College of Law and holds a master's degree in public administration with a minor in health care administration from Drake University. She can be reached at [Annette\\_Miller@hipaanswers.com](mailto:Annette_Miller@hipaanswers.com) or 952-400-1100.*