



HIPAA e-Rule Surprises Small Businesses

Many small companies will fail to meet this week's compliance deadline for protecting employee health data stored on computers.

[Marie Leone](#), CFO.com | US

April 20, 2006

U.S. law has protected the privacy of employee health data since 1996. But until last year, the appearance of that data on company computer screens was mostly protected by rules of thumb, like so-called "cleaning woman" and "shoulder surfing" policies. In both cases, company policies generally encouraged employees to keep confidential information from the wandering eyes of maintenance workers and colleagues by tilting a computer screen or using a glare filter to block the data displayed on a screen. But that's no longer enough.

In 2003, an addendum was slapped onto the Health Insurance Portability and Accountability Act of 1996 (HIPAA) addressing the security of electronic "protected" health information — that is, confidential employee health data stored in databases, computer documents, and in e-mail messages. Large companies had to comply with the new security standards as of April 2005. On Friday, April 21, small companies will have to do the same. According to experts, few will be ready.

Issued by the U.S. Department of Health and Human Services (HHS), the HIPAA Security Rule mandates that companies with small health plans — defined as those with less than \$5 million in group medical claims — will have to comply with 17 standards, and at least half of the 41 security specifications contained in those standards.

In general, the rule requires companies with self-insured or fully-insured plans to maintain the confidentiality, integrity, and availability of employee health data. Yet, many small company executives are unaware of their new responsibilities, says Eric Raymond, CEO of insurance broker Corporate Synergies Group (CSG).

Raymond cites a recent CSG survey of 235 small companies based in the New York tri-state area to illustrate his point. As of April 17, only two of the companies surveyed were in compliance with the new regulation. Additionally, only 28 companies are expecting to meet Friday's deadline, while the rest said they would fail to meet the compliance target date.

More worrying, one third of the non-compliant companies said they would miss the deadline because they were unaware of the rule. "When I visit small company clients and mention the HIPAA security rule, I get blank stares and shrugs," says Kevin O'Hara, CSG's director of compliance.

Other survey respondents claim that they will fail to comply with the rule for a variety of reasons, including not making compliance a priority, having too many other regulatory issues to focus on — especially Sarbanes-Oxley Act compliance efforts, and lack of resources to complete their HIPAA compliance program. The companies surveyed in the CSG study ranged from 100 employees to 1,000 employees.

Implementing the new security measures should not be as onerous for smaller companies as it was for larger ones, reasons O'Hara, mainly because smaller companies tend to have less data, and therefore less complex information technology systems. Nevertheless, compliance and IT managers have their work cut out for them.

Although the rule does not mandate specific compliance technology, it does list basic requirements. At a minimum, companies have to name a security officer to oversee the implementation of the regulation, identify and document security policies and procedures, conduct a risk assessment of the company's health information systems, and document and fix any vulnerability the assessment uncovers. In addition, all companies have to draw up "business associates agreements" to assure that third parties that have access to the information, such as plan administrators or computer repair vendors, will appropriately safeguard the data.

Small company managers shouldn't panic yet, because the rule was written with them in mind. Taking into account the compliance burden small companies will face, the rule applies the "scalability principle" to its mandates. Essentially, all 17 standards must be met, but only 20 of the 41 specifications within the standards are required. The other 21 are "addressable," which means companies — big and small — have the flexibility to determine whether the specification is "reasonable and appropriate" for their circumstances, and whether a standard can still be met by way of an alternate route. Most large companies will wind up implementing most of the specifications, but smaller companies may be able to work around them.

For instance, companies with a relatively small workforce, say 25 employees, may not find it necessary to install card-key systems or other building access systems to comply with the rule's facility security plan standard. That same company may not deem it necessary to meet the access control standard by implementing encryption and decryption programs on their IT systems.

The rule's flexibility only extends so far, though. **Penalties for non-compliance are applied across the board, regardless of the company size.** On February 16, almost a full year after the large company compliance deadline, HHS gave the security rule teeth, and issued final enforcement regulations. **Civil fines run \$100 per day, up the maximum of \$25,000 per standard, per calendar year. Thus, a four-standard violation could cost a company \$100,000 in annual penalties.**

Criminal penalties are less likely, says O'Hara, although breaking into systems and then stealing and selling social security numbers, for example, would clearly bring criminal charges and jail time if the individual was convicted.

The likelihood that HHS will come down hard on rule violators within the next few months is less clear. O'Hara says it's too soon to tell how violations will be treated, but he expects that **the agency will take into consideration whether a good faith effort is being made to comply with the standards.** On the other hand, HHS may be looking to show its teeth, and make an example out of the first batch of rule-breakers it catches. But that may not be easy.

Unlike other agencies, such as the Internal Revenue Service, HHS does not have the authority to audit companies as a way of ferreting out violators, explains Raymond. A formal HIPAA complaint has to be filed with HHS before the agency can start an investigation.

That process brings up another rule of thumb. **The "one, former disgruntled employee" rule,** quips O'Hara. **All it takes to spark a federal probe, he says, is a single former employee who feels wronged by the company.**