Health Information Compliance Alert

Security PROGNOSIS FOR COMPLIANCE NOT A WAIT-AND-SEE MATTER

Sure, there's no compliance deadline to fret over regarding HIPAA's security rule yet but if preparation for the privacy rule taught you only one thing, it's that getting a head start is crucial.

The White House's Office of Management and Budget staff fessed up Jan. 13 with charmingly bureaucratic laconism that it has received the Health Insurance Portability and Accountability Act's final security rule. The OMB notice reads: "HHSCMS RIN: 0938-AI57 Health Insurance Reform Security Standards (CMS-0049-F) STAGE: Final Rule. ECONOMICALLY SIGNIFICANT: No. RECEIVED: 01/13/2003."

What the OMB intends to do with the rule is anyone's guess not to mention when it anticipates releasing the final rule to the public but there are a few steps covered entities should be considering now that will help to prepare them for the imminent advent of the final rule.

The OMB likely will surgically extract whatever it deems to be malignant provisions of the security rule, but you shouldn't sit idly in the waiting room for the results of this procedure. If you haven't done so already, there are a few steps you can take to ensure you get a head start on security rule compliance:

No need to start from scratch. Remember that there is an archetype for the administrative requirements pertaining to HIPAA security, and that you've probably already taken steps, whether you know it or not, that will aid you with security compliance implementation: following privacy rule guidance.

Covered entities must take all "reasonable" steps to protect a patient's protected health information. Until the OMB issues the final security rule, "the draft of that rule provides the CE with guidance that can help define what 'reasonable' means," explains Donald Ribelin, HIPAA Project Manager with FirstHealth of the Carolinas.

Ribelin says he considers it "reasonable" for CEs to develop their policies based upon the recommendations in the draft of the security rule. "At the very least," he notes, "you'll be taking positive steps toward compliance."

Conduct a security assessment. Even though there's no firm deadline for the security rule, this should be your first step. Your computer and software vendors should be able to help you perform an internal assessment and identify any deficiencies. Vendors and consultants can also advise you which software to use, and which procedures best fit your organization.

Psst...What's The Password?

Restrict password access. Sometimes covered entities that have provided passwords to their staff discover too late that those passwords are being shared, according to Jennifer Bever with consulting group KarenZupko & Associates Inc. (KZA) in Chicago.

One way to implement more secure daily operations is to ensure that staff members don't share their passwords, and that the passwords are difficult to decipher, KZA advises.

And the number of characters your CE uses may depend on the particular platform you use. For instance, if you're on a Microsoft platform, you should probably use seven or eight characters, and if you're on UNIX, it's usually eight, says Fred Langston, senior principal consultant with Guardent's Seattle office.

Utilize a password aging plan. Langston tells Eli CEs will need to have a password aging mechanism, and he advises CEs to have staff members change their passwords every 35 days, and at least after every 90 days.

Langston says for small offices such as physicians' practices, an onerous password policy is unnecessary, "but you also want to have a complexity requirement a mixture of letters, numbers, special characters, upper and lower cases," he urges.

Implement access controls. Implementing fundamental access controls is an area that will not be made obsolete quickly. A provider should think about what logical steps it can take to minimize access risks, including unauthorized external individuals accessing the provider's system or internal users having access to sections of the system that are unnecessary for the individual's job requirements. Users should be restricted to the level of electronic information that is necessary for performance of their job functions, says Eileen Kahaner, an attorney in the Washington office of Arent Fox Kintner Plotkin & Kahn.

A provider should "prohibit staff from taping passwords to the outside of their computer monitors and/or otherwise sharing this information," she urges.

"Someone at the practice also should be responsible for immediately terminating access rights to individuals who leave the organization. Everyone should be required to log off their machines at the end of the day," Kahaner informs Eli.

Develop an encryption solution. This is high on Langston's list for small providers. If you're encrypting data at risk on your system as well as data in transit, you're pretty much covering all bases in terms of data protection. That'll help out a bunch if the feds ever come banging on your door, since protecting health data puts smiles on regulators' faces, he claims.

Perform a data classification. If you don't know where your patient data lives, how can you protect it? Langston says he's spoken with many CEs who claim to have performed a gap analysis, but don't know the first thing about how their data is classified.

Performing a data classification means evaluating the processes involved in storing, moving and accessing your protected health information. Langston says CEs "commonly think this is the same form of classification that corporations or military use top secret, highly classified, trade secret, etc. but for HIPAA the goal is to identify PHI."

Langston says the most important point to take away on classification is if you can't locate every place where PHI data is stored, transmitted or received, "you're not ready for a gap analysis, let alone implementation of remedial measures," so make sure you get this taken care of ASAP, he urges.

While it's still too early to say what form security rule enforcement will take, taking these due diligence steps should provide a springboard to compliance. And if you document each step you make, you'll be taking a giant leap away from any potential enforcement actions.