Health Information Compliance Alert

AccreditationMin GOT PRIVACY ACCREDITATION? URAC WANTS TO HELP

Well, they promised it, and now they've delivered. Accreditation corporation URAC hopes to steer covered entities into privacy rule compliance, but first they want you to comment on their proposed standards.

Last month, URAC announced it was preparing privacy and security rule compliance standards intended to serve as a guideline for CEs and others seeking accreditation (see HICA, vol. 3, no.1, pp. 4-5). As promised, URAC released its standards Feb. 10 for public comment.

While the corporation says the standards represent only an outline of the process by which it will evaluate CEs' privacy rule compliance programs, URAC claims these standards will allow CEs and all other organizations for whom compliance with the Health Insurance Portability and Accountability Act is necessary to demonstrate they've adopted policies and procedures that ensure the privacy of health information in accordance with the privacy rule.

"The purpose of this accreditation program is to verify that an organization has put in place the necessary infrastructure and implemented the necessary processes to comply with the HIPAA Privacy Rule," said Garry Carneal, URAC president and CEO.

Some of the requirements URAC will look for when determining an organization's accreditation merit include:

- appointment of a chief privacy official who is responsible for the organization's HIPAA compliance program and other ancillary policies and procedures;
- completion of a comprehensive self-assessment focused on how protected health information is stored, used and disclosed;
- appropriate policies and procedures designed to address physical, technical and administrative safeguards to protect (and maintain the security of) the privacy of PHI, including controls on access to PHI that provide the minimum amount of access necessary for staff members to perform their jobs;
- policies and procedures to mitigate the harmful effect of any use or disclosure of protected health information in violation of HIPAA or its own privacy practices; and
- policies and procedures for maintaining proper documentation of PHI-related transactions for six years, among other requirements.

Privacy rule accreditation also calls for proper maintenance of policies and procedures. The organization must maintain master lists of all policies and procedures, must review those policies at least annually, and is required to revise any out of date systems.

The program also addresses issues such as workforce training, the rights of individuals under HIPAA, notices of privacy practices, authorizations, complaints, business associate agreements, and takes into consideration the disparate dynamics of specialized groups, such as group health plans, affiliated CEs, hybrid entities, and others.

The first step toward accreditation will require the CE to perform a self-assessment test to ensure whether the it has an effective HIPAA compliance program in place, says Guy D'Andria, URAC's senior VP of standards development.

Next, URAC requires them to put together evidence of their compliance program, including copies of their policies and procedures that they've implemented to meet the various requirements of the privacy rule, to provide job descriptions of HIPAA personnel such as their privacy officer or other key staff, and to generate evidence that they've trained staff in their responsibilities that have access to PHI.

"We would review that documentation looking for any gaps, and we'd have a dialogue with that company about those

gaps so that they'd have an opportunity to fill them," D'Andria tells Eli.

Once that process is complete, URAC goes on site and conducts a review of the CE's actual operation, observes how they manage PHI, and talks to staff who have access to PHI to make sure they understand their responsibilities. If they pass that stage of the process, they go to an accreditation committee, D'Andria explains, which has the final say whether or not to grant accreditation.

URAC is quick to note that the standards will not ensure compliance with the privacy rule. Rather, accreditation will send a message to regulators that accredited organizations are displaying a commitment to the privacy rule.

The public comment period for the program ends March 12. To see the standards, go to http://www.urac.org/hipaapstds10.pdf.

Editor's Note: URAC says it prefers to receive comments by e-mail at comments@urac.org (with the subject line reading "Comments HIPAA Privacy Standards"), but says comments may also be mailed or faxed to: URAC, Attn: Public Comments HIPAA Privacy Standards, 1275 K Street, NW, Suite 1100, Washington, DC 20005; the fax number is 202-216-9006.