Health Information Compliance Alert

Transactions: TCS TESTING PLAN VITAL TO ENSURE YOUR BUSINESS' SURVIVAL

4 Tips To Help Avoid Enforcement Watchdogs And Lost Revenues

If you haven't begun testing your solutions for compliance with HIPAA's rules on transactions and code sets (TCS), you could easily find yourself out of business when claims aren't paid.

HIPAA's privacy and security rules usually garner the most publicity when it comes to covered entities' compliance concerns, and the TCS standards are considered by some to be HIPAA's abandoned stepchild. Those of you who filed compliance extension requests back in October were permitted to put off testing your solutions for implementation of the TCS standards until April 16 of this year.

The **Department of Health and Human Services** recently said it plans to take a flexible approach with respect to TCS enforcement. While that's good news for most entities struggling with the regulation, your major concern should not be with the **Centers for Medicare and Medicaid Services** coming down on you, but rather with your survival as a business. Potential enforcement by the CMS is not as significant as your livelihood. After all, "come October 16, if you're not transmitting electronically to Medicare, you're not getting paid," warns **John Yates**, a principal at **Phoenix Health Systems** in charge of strategic planning.

For those of you who failed to begin testing by the required April 16 date, you must start A.S.A.P. It's not too late to get moving, but the clock is ticking, and the race is on. Here are some of the most significant and easy-to-implement steps you can take to comply with the TCS standards:

1. Assign responsibility for testing. Your privacy officer won't have much, if any, input when it comes to testing your solutions for TCS implementation, and you'll need to find someone who has loads of tech experience for this task.

For larger facilities, you should coordinate your testing phase with your IT department. For smaller entities, strongly consider outside consulting help. "A lot of my clients are small providers who probably couldn't afford to have the IT staff necessary to do this in-house," says **Robert Markette** with **Gilliland & Caudill** in Indianapolis.

If you do go out of house, Markette says entities have a few options: "You can buy software, you can tell your IT people to start working on the problem, and in the meantime you can switch to using a health care clearinghouse that is compliant and do that for the interim period until your IT guys have the problem fixed and you are compliant." Whichever path you choose, make you sure you appoint someone - and preferably, have more than one person working towards your goals - to drive this process on internally.

2. Communicate often with your vendors. Software vendors are vital to TCS compliance. After all, your vendors are making the products that will ultimately make you compliant and will ensure proper, efficient electronic transactions. You must receive concrete evidence from your software vendors that the software you're using or planning to use has been upgraded and it now definitely has the capability of transmitting and receiving the standard transactions, advises **Randa Upham**, Principal at **Phoenix Health Systems** in charge of Program Development and overseer of Phoenix' e-learning services.

If your software can't transmit claims in a HIPAA standard format, find out if and when your software provider will be able

to produce an upgrade. By this point vendors already should be in their testing phase so their customers have time to familiarize themselves with the new software, says **Nileen Verbeten**, vice president of the **California Medical Association**'s Center for Economic Services.

Verbeten tells **Eli** she created two simple letters for CMA members: One letter was intended for the member's software vendor; the other was to go to the member's billing service, if it used one. The letters ask if the software the CMA member is currently using is HIPAA-compliant. If it isn't, it asks what the physician has to do and what it will cost. The letters take a practical approach: "Don't give me all this mumbo jumbo about all this technical stuff, just tell me what I have to do," Verbeten explains.

3. If necessary, use your clearinghouse. "A lot of vendors are saying, 'We suggest you contact a clearinghouse in the meantime'" until they product a software upgrade, says Yates. He says that's a good route to take and says in many cases clearinghouses are a great resource for making your transactions compliant.

Well, a clearinghouse is certainly an option and most providers use some kind of clearinghouse anyway. However, you've still got to give them the data elements to create the 837 claim form, he warns. "The problem is, this is everyone's fallback solution, and everyone's waiting because they don't want to incur the expense," he notes. If you are going to use a clearinghouse, do it now, since clearinghouses are likely to be flooded with requests like this, and they may not be able to provide services as quickly as you'd like.

4. Don't listen to the rumors. There has been much speculation of late that CMS, the agency responsible for TCS enforcement, will issue another extension for entities who fail to become TCS compliant by the October 16 deadline. Fueling these rumors is the notion that CMS will not permit entities to suffer a massive and chaotic financial disaster come October and will provide entities with additional time to comply with the standards. "I think what people are grabbing on to is a fervent belief - or a hope and prayer - that CMS will come out and issue another extension. A lot of people are hoping that will be the case, because they are aware of the seriousness of it, and they don't see how they can get there in light of where we've gotten to in July," says Upham. But don't count on a reprieve, the experts warn, and continue to work as if no extension will be provided.

Editor's Note: For more HIPAA help, including further aid with TCS compliance, check out the CMA's Web site at
www.calphys.org/html/hipaa_help.asp
 and Phoenix' HIPAA resources at www.hipaadvisory.com.