Health Information Compliance Alert

Add These 5 Measures to Your Compliance Checklist

Check your state's provisions to make sure you're up-to-date.

If your state's laws regarding privacy are more stringent than those under the HIPAA Privacy Rule, following the HHS Office for Civil Rights (OCR) guidance will do your facility more harm than good. And even though it may seem like an extra step in compliance planning, it is essential for you to review and integrate your state's requirements into your protocols on protecting and securing patients' protected health information (PHI).

"Luckily, a good job with HIPAA compliance can provide a good framework for compliance with all of the state laws an entity could be subject to," says **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC** in Charlotte, Vermont.

Put these five extra steps in your plan to ensure you're compliant with state regulations:

- "Coordinate a review of applicable local laws," advises Sheldon-Dean.
- Check with your EHR vendor to ensure state requirements are met as well as federal ones.
- Analyze the differences between state and federal rules for encryption, breach notification and timelines, and personal information, covering both sets of standards in your plan.
- Evaluate and implement state policies that protect specialty-specific sensitive information that may extend beyond HIPAA.
- "Add the necessary pieces and changes to your existing privacy and security policy and procedure set," stresses Sheldon-Dean.

It's better to be safe than sorry and cover all your bases in regard to your state's laws. "Many of these rules call for the same precautions, safeguards, and procedures, and it's better to make your existing privacy documents more robust instead of creating parallel policies and procedures for each rule or law," Sheldon-Dean explains.