# Health Information Compliance Alert

## Security: Depend On Dummy Data To Protect PHI During System Tests

**Use this advice to ensure your patients' information gets used only when necessary.**

If you're using your patients' PHI to develop and test new software geared toward smoothing your operation's wrinkles, you could be setting yourself up for a privacy and security violation.

"Development environments are much less secure than other environments, making it easier to steal or expose somebody's information," says **Fred Langston**, principal consultant with VeriSign in Seattle.

Follow this advice to keep your work with PHI secure in less-protected environments:

**1. Use Fake Data When Possible**

You do not need to use PHI in the beginning stages of software development, explains David Szabo, an attorney at Nutter McClennen & Fish in Boston. "We used dummy test data to work out the kinks during the first level of testing," Szabo says of his experience working with a client who created homegrown information management software.

"There is no reason to use real PHI in a development environment," Langston concurs. Why? There are many people involved in the initial stages who have no need to see your patients' PHI. And because the testing environment is insecure, it's almost impossible to justify exposing patients to that risk, he says.

**2. Use Authorizations To Introduce PHI**

In the more advanced stages of application testing, it can be very helpful to conduct tests with actual data. "There are some conditions that are hard to re-create using fake data or a limited data set," such as twins with similar names or a name with nontraditional characters like accent marks, Szabo says.

**Good idea**: You don't have to bring in patients' data to accomplish this testing. Ask your technology staff members or other employees who understand the importance of this project to sign an authorization allowing you to use their PHI, Szabo suggests.

**Important:** Protect yourself and your personnel by outlining the scope and timeline for this project before you access their PHI. You should also develop a plan for how you'll end the testing -- for example, you may decide to allow access for a two-week period and then sever that access automatically at the two-week mark.

**3. Define Need-To-Know**

If you have to use PHI to ensure your new applications will work in day-to-day operations, you must limit the staff members who have access to the data, Langston notes.

**Example:** Your entire technology team worked for the past month to get the application to a nearly complete state, but you need to fix one recurring problem. Designate one or two testers to work with that problem and have access to actual patient information.

**Remember:** You also must abide by the minimum necessary rule during the testing, Langston points out. "Your staffers should never have access to the entire medical record if they only need a portion of it to do their jobs," he says.

Your first step is to define what you'd consider 'need to know' and 'minimum necessary' in the testing environment, and then document how you will allow and remove access.

### The Bottom Line

With the increasing number of companies going belly up after disastrous security breaches, you cannot afford to use confidential information in situations where you cannot guarantee that the data will remain protected.