# Health Information Compliance Alert

## Get Expert Help For Your Security Policy

**Follow the right framework to create and update your policy.**

As you wade through the murky waters of HIPAA Security Rule compliance, your security policy should not only chart your voyage, but it should also serve as your lighthouse for when you drift off-course. But for your security policy to become such a vital and reliable document, you need to first understand the framework for all that the policy must include.

According to HIPAA expert Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, VT, your basic security policy framework should look like this:

**Four Basic Policies (or Policy Types):**

1. Security Management Process
2. Information Access Controls
3. Data Management (Contingency-Backup-Retention)
4. User Policy

• Include enabling language in your policy.
• Define details in your procedures.
• Include as much documentation as possible.

Enlist These Resources to Ensure a Compliant Security Policy

And if you need help drafting your security policy or ensuring that it remains compliant, Sheldon-Dean points out that you can get help from the following resources:

**The SANS Institute's Security Policy Project:** Includes a short primer for developing security policies, along with samples and guidance. Read more at www.sans.org/resources/policies.

**New York University HIPAA security policies**: Provides model security policies with a good level of detail, and many of the concepts are directly transferable. Read more at www.nyu.edu/its/policies/#hipaa.

**The National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (SP 800-61 Revision 2):** Provides a practical guide to responding to incidents and establishing a computer security incident policy and process. Read more at csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

**NIST ITL Bulletin (September 2012):** Focuses on the revised SP 800-61. Read more at csrc.nist.gov/publications/nistbul/itlbul2012_09.pdf.