Achieve.Illustrate.Maintain.
Compliance *Simplified*

5 Key Steps of HIPAA Compliance

In a recent interview with Beckers Hospital Review, Our CCO Bob Grant highlighted what is necessary for healthcare providers to achieve, illustrate and maintain HIPAA compliance in 5 easy to understand steps.

1. **Perform a "true" risk analysis.** To understand system vulnerabilities, healthcare providers have to do an internal risk analysis or hire an outside auditor to perform a risk analysis for them. To perform a "true" risk analysis, the provider has to be able to say "no, we don't comply with a certain part of the regulation," says Mr. Grant. Although many healthcare providers are hesitant to admit they are not HIPAA compliant, honestly answering risk analysis questions is necessary to ascertain what a system's weaknesses are, adds Mr. Grant.

2. **Have a remediation plan**. Healthcare providers need to use the information from the risk analysis to develop a plan to resolve its vulnerabilities, says Mr. Grant. Along with the remediation plan, providers also need to track the documentation that shows the non-compliance issue was fixed. There are tools available that help providers track the documentation, and healthcare systems with multiple facilities should utilize the tools to simplify the process, adds Mr. Grant.

3. **Have vendor management protocols.** Healthcare providers need to have a valid business associate agreement in place with all vendors they are sharing patient information with, says Mr. Grant. Providers should send vendors a HIPAA security audit to ensure the vendor is in compliance with the HIPAA security rule. It is important for healthcare providers to address all vendor non-compliance issues because "if you act like an ostrich and put your head in the sand, HHS will come down on you hard," adds Mr. Grant.

4. **Update documents**. The HIPAA omnibus rule requires healthcare providers to have a manual containing current policies and procedures addressing each part of the omnibus rule — such as business associate agreement monitoring and sanction strategy. Providers' policies and procedures must be updated "periodically," and it is good practice to update with federal government rule changes or every two years, says Mr. Grant. "You may not have to change the manual when it's reviewed, but you at least have to review the policies and track that you did by at least changing the revised date," adds Mr. Grant.

5. **Have an incident management plan.** "Everyone has a security incident, it's the nature of healthcare, and security incidents can happen at any organization," says Mr. Grant. The healthcare industry relies on phones, fax machines and other electronic devices that are often compromised and lead to data breaches. As an incident response measure, healthcare providers need to keep accurate records — such as employee HIPAA training documents and audit logs — to determine what information was compromised during a breach and to be able to track the incident to the responsible party, adds Mr. Grant.

-Bob Grant, CCO at **Compliancy Group** and former HIPAA auditor

Compliancy Group