# Health Information Compliance Alert

## HIPAA Compliance: Take 7 Steps to Protect PHI 'In the Cloud'

**Choose your vendor carefully -- or risk leaks.**

If you're like many other healthcare providers, you're either currently considering or possibly already using some kind of online or cloud storage for your medical files. Although cloud storage is economical and convenient, it's rife with risks and gaping security holes. That's why auditors are increasingly focusing their attention on protected health information (PHI) online and in the cloud.

You can avoid many problems with cloud storage by simply selecting the right kind of vendor and executing a contract in compliance with HIPAA rules and related regulations. Experts offer the following steps for staying out of hot water while you're transitioning to the cloud:

**1. Evaluate the Vendor**

When it comes to cloud storage, not all vendors are created equal. Choose "a vendor with experience in dealing with regulated information, ideally protected health information," advise **Jim Wieland** and **Joshua Freemire** of **Ober Kaler Attorneys at Law**, a Washington, D.C.-based firm specializing in regulatory healthcare law. A cloud-storage vendor who has experience in dealing with HIPAA security requirements will understand your need for HIPAA-specific mechanisms.

**2. Check Out the Data Protection**

Ask about the level of encryption the vendor will apply to PHI in the system. But beware that "not all vendors are willing to deploy encryption if most of their users do not require it," cautioned Wieland and Freemire in a recent blog post at oberhealthinformationtechnology.com. Also ensure that the vendor has appropriate barriers and protections in place to segregate your data from the data of the vendor's other clients.

**3. Ensure Proper Breach Protocols**

When you're evaluating a potential cloud-storage vendor, you must consider what level of breach monitoring the vendor provides, said Wieland and Freemire. What is the vendor's breach response plan? What are your monitoring responsibilities versus those of the vendor? (See page 90 for more information on breach protocols.)

In some ways, you may feel like the security of your PHI is completely in the vendor's hands -- and you're right. "A provider may have to take on faith in some respects that [the vendor] can live up to that provision" of privacy and security verification, says **Wayne J. Miller, Esq.**, founding partner of the **Compliance Law Group** in Los Angeles. But really this is where your Business Associate Agreement (BAA) comes in -- you must have in writing the vendor's responsibilities and your expectations of how the vendor will protect your patients' PHI.

**4. Develop a BAA**

In most cases, your cloud-storage vendor qualifies as a Business Associate (BA) and should enter into a BAA contract with you. Beware of any vendor who does not want to sign a BAA, or those who may claim that they are not in fact a BA.

In the BAA, include the essential language, such as the vendor "shall use reasonable and appropriate safeguards" for PHI, Miller says. Your BAA should also outline breach reporting requirements and compliance standards for any subcontractors.

Several larger vendors, such as Microsoft Office 365, have developed "canned" BAAs and a check-off option where Microsoft agrees to abide by HIPAA under the BAA, Miller notes. But keep in mind that off-the-shelf storage may need

HIPAA tweaks and special access controls to stay in compliance, he warns.

**5. Monitor Compliance**

You must provide oversight of the vendor's cloud storage activities, typically by your privacy and security officers, Miller states. Just because you have that BAA doesn't mean you're simply immune to the vendor's potential screw-ups. A breach -- even if it's clearly the vendor's fault -- will still fall back on you as well, because under the Health Information Technology for Economic and Clinical Health (HITECH) Act, both the covered entity (CE) and the BA are liable.

Under HITECH, the BA has virtually the same requirements as the CE in terms of security. With privacy, BAs must have "reasonable safeguards" to prevent inappropriate access to PHI and "to protect the privacy of the information they're maintaining," Miller explains.

**6. Update Your Policies & Procedures**

One of the most important compliance elements for cloud computing is to "make sure the 'paper' is in order," Miller says. Your policies and procedures must specifically speak to your online activities and how you'll ensure protection of PHI in the cloud.

**7. Audit Yourself**

Conduct self-audits, run-throughs and "fire-drills" to gauge your own HIPAA compliance, specifically in terms of your online cloud computing, Miller recommends.

Among other things, you will need to decide who will have access to the PHI stored "in the cloud" and at what level of access, Miller says. For example, a physician would perhaps have "Level 5" access, while a receptionist would have "Level 1" access. And then you have the issues of authentication, meaning what kind of passwords or access barriers you will need to ensure that the PHI isn't at risk for unauthorized access.

In your self-audit, you must also look at your vulnerabilities when using online cloud services -- perform a detailed risk assessment and document your steps to mitigate those risks, Miller stresses. When an auditor comes knocking, you need to show that you've thought about where all your vulnerable spots may be and how you'll safeguard those areas.