

# Health Information Compliance Alert

## Case Study: Backup Devices: Learn 3 Crucial Lessons From The Latest Data Breaches

**Why encryption is well worth the cost, especially with flash drives.**

Flash drives, or "thumb drives," and other similar backup media devices are handy because they're very small but can store an amazingly large amount of data. However, what makes flash drives so convenient are the same characteristics that make them so dangerous when it comes to HIPAA breaches.

### **Beware: Convenient Storage May Equal Easy Theft**

**Background:** Two recent large-scale HIPAA breach cases involved unencrypted backup devices. One case, involving the Indiana oncology practice **Cancer Care Group**, stemmed from a breach caused by the theft of an employee's computer and unencrypted backup media device, according to a Sept. 3 report by the law firm **Nixon Peabody LLP**.

The backup device contained 55,000 current and former patients' names, addresses, birthdates, Social Security numbers, insurance information, and clinical information. As a result of the breach, Cancer Care entered into a settlement agreement with the **HHS Office for Civil Rights** (OCR) that included a \$750,000 fine and a corrective action plan to remedy deficiencies in its HIPAA compliance program.

The second breach case involved **Lawrence General Hospital** and a missing flash drive that contained patients' names, lab testing codes, and slide identification numbers.

But you don't have to suffer the same serious consequences as these healthcare providers, even if you choose to use flash drives. Here's what you need to do to protect your backup media devices from costly HIPAA breaches:

### **1. Use Encryption Flash Drives**

If you need to save PHI on flash drives, you should employ safeguards like using encryption flash drives or password-protected flash drives, according to an Aug. 24 blog posting by attorney **Mary Beth Gettins** of **Gettins Law**. Also, do not store or send passwords with the flash drive.

Encryption is not always cheap, but it's worth it, said **Thomas Lewis, CISSP, CISA, QSA**, Partner-in-Charge of **LBMC Information Security** in a recent analysis. "Robust encryption can insulate you from HIPAA fines and provides an added layer of security that helps foster trust with your patients — making the investment for encryption well worth the cost."

### **2. Track & Inventory Your Flash Drives**

Another important safeguard you can employ is to track and inventory your flash drives, Gettins advised. You should also prohibit or restrict what PHI your staff members may save to flash drives.

### **3. Beef Up Your Data Management Policies**

You can't always control what your employees are doing, but you can mitigate risks "by putting security systems in place to help keep users from doing improper things with data," Lewis stressed. "To make sure patient information is secure, organizations need to develop strong data management policies to minimize healthcare data breaches."

**Example:** Some networks will allow a physician to download patient data to **Dropbox**, Lewis noted. "That's a big no-no."

This is also where training and education come into play. "Instead of just telling doctors not to use Dropbox, explain why it is harmful," Lewis suggested. "For all the stories of sophisticated hackers, data is typically put at the most risk by ordinary employees being careless or ignorant to the risks." That's why you should be proactive and provide staffers with secure tools to achieve their objectives so they won't resort to unsafe methods that put patient data at risk.