HIPAA Security and Privacy

It is critical that your LHD establish controls and checklists to protect itself from any HIPAA breaches. With employees having access to both internal and external systems, it is important to maintain organized processes for providing accesses upon hire, and deactivating accesses at termination.

Following the guidelines described below consistently can protect your LHD from compromising unsecured protected health information. Remind your staff that carrying out these steps promptly and consistently is not a reflection on the separated employee, and it is not a matter of distrust. It is a matter of respecting the integrity of your data systems and ensuring you have been vigilant in protecting them.

- **Assemble** a **list of all *internal* systems your company controls access to.** This includes your practice management system, EMR, accounting and payroll packages, network, and e-mail systems to name a few. Have all of your department managers help you develop the list, to ensure you identify every system.

- **Assemble a list of all *external* systems your company accesses via the Web,** or via other secure means. Again, brainstorm with every department to assemble this list. You might be surprised to find that if your maintenance staffer quits, no one could log in to schedule your next inspection of your heating and cooling system.

- **Create a "user-access checklist,"** which includes a checklist of all of the systems you have collected above, a place for "employee name," "hire date," and "termination date."

- **When you have a new hire, create a copy of the checklist and put her name on it.** Record every system you provide access to for this new hire. File the completed checklist in her personnel file.

- **When you provide additional access, or remove access for an employee, update the checklist** in their personnel file. During employee annual reviews, ask the employee if they still need access to each system. Perhaps an employee has changed departments, and no longer requires access to a system. Change the access, and updated their user-access checklist.

- **When an employee separates, pull out the user-access checklist from their file.** Immediately deactivate all internal accounts and contact all external parties to disable all access to external systems.

- **Ensure you have at least two separate authorized employee users on every account** for all of your external systems, which could include anything from your online bill payment system for the electric bill to the username and password for your company credit card's Web site. This will ensure that if one of them is released, the external company will still talk to the other authorized employee for whom you also set up an account.

- **Keep these records stored and formally maintained.** Often, these records are maintained by accounting departments, HR departments, IT, or a central office administrator.