Handling Employee Health Information: Protect and Secure

Common sense dictates that you do not share private medical information except with those who have a need and a right to know it. Common sense does not always prevail – especially if an employer has not set up policies and procedures to ensure that health information is protected.

For employers that are uncertain how best to protect health information, the following are some action items for major areas of an employer's operations, taking into account HIPAA and the other federal laws protecting health information. No checklist can be completely comprehensive, but this list can provide a starting point for guarding against the inadvertent disclosure of private information with its all-too-common legal and other consequences.

Web sites

- Once you have a website, some documents must be posted on it, such as the HIPAA privacy notice.

- If employees can access their health plan enrollment information, flexible spending account (FSA) claims information and dependent care spending account information through the employer's website, make sure that access is secure and private.

- Tell employees not to disclose their passwords to anyone.

Booklets

- Make sure the HIPAA privacy notice, or at least a summary of it, is included in all summary plan descriptions.

- Include a reminder about the privacy notice in the plan's open enrollment booklets every year, to ensure that the plan meets the three year reminder requirement.

- Have a clear statement in employment booklets detailing when and to whom employees should submit the medical certification forms required by the Family and Medical Leave Act or other employer programs such as sick leave. Make sure that employees are not required to submit detailed private health information to their supervisor or manager.

Human Resources

- Ensure that human resources staff is aware of their roles and the type of health information they are permitted to use in that role.

- If a HIPAA firewall is in place, conduct regular training to remind staff of the distinction between group health plan functions using PHI and employer functions using other health information.

- Take identifiers, particularly social security numbers, off routine communications to employees. Do not require employees to provide SSNs to human resources staff unless necessary.

For more information, contact CTSI at 303-861-0507.