

MORE ON COMPUTER FILE DESTRUCTION BY YOUR EMPLOYEES

Waldthausen & Associates, Inc. is a Retained Executive Search firm with the focus on recruiting managers that influence a company's result and earnings. The firm focuses on recruiting professional managers for US subsidiaries with parent companies located in central Europe.

Employer Can Sue Employee for Computer File Destruction

In many cases when an employer is preparing to terminate an employee, concerns arise over that employee's access to the business' computer files, and possible damage that the employee could do once notified of the termination decision. In addition to the usual preventive measures, a recent decision from the Seventh Circuit Court of Appeals adds a new measure for seeking compensation from an employee who engages in electronic vandalism. The case was filed by a commercial real estate company against a former employee who was provided with a company owned laptop computer. The employee quit to start a competing venture, and prior to returning the computer, deleted vital company information. He installed a secure-erasure program designed to prevent the company from recovering the deleted information.

The employer sued the former employee under the federal Computer Fraud and Abuse Act (CFAA). CFAA was intended to punish computer virus creators by prohibiting the transmission of any program or code that causes damage without authorization to a protected computer. The defendant claimed that he had never "transmitted" any file to the laptop computer. The Seventh Circuit reversed a lower court decision for the defendant, holding that loading of the secure-erasure program onto the computer constituted transmission under DVAA.

CFAA will not apply in all cases where an employee or former employee engages in electronic misconduct. If the employee had used the computer's existing programs to attempt to delete the information, there would not have been a CFAA transmission. Also, much of the court's determination regarding the defendant's authorization to load programs onto the computer was based on his legal duty of loyalty to the employer. In states such as North Carolina that do not recognize a duty of loyalty to employers, CFAA claims may be more difficult to prove in the absence of clear rules regarding computer use.

CFAA contains strong criminal as well as civil penalties. In addition to using this statute, employers concerned with employee access to computer data should take serious measures to protect this information. The steps can include blocking problem employees from sensitive data, use of strong confidentiality provisions in handbooks and in individual agreements with employees provided access to sensitive data, and clear rules governing the use of company-owned electronic equipment. Given the potential for harm unauthorized destruction or misappropriation of electronic information can cause, good risk management practices require attention to these issues before a crisis arises. (Parker Poe Adams & Bernstein LLP)

Permissible HIPAA Disclosures on Beneficiary's Behalf

The Department of Health and Human Service's Office of Civil Rights has recently provided guidance concerning the conditions under which health plans may disclose protected health information to a person who calls the plan on the beneficiary's behalf.

In general, the HIPAA Privacy Rule permits a health plan (or other covered entity) to disclose to a family member, relative, or close personal friend of the

individual (plan participant), the protected health information (PHI) directly relevant to that person's involvement with the individual's care or payment for care. A health plan also may make these disclosures to persons who are not family members, relatives, or close personal friends of the individual, provided the health plan has reasonable assurance that the person has been identified by the individual as being involved in his or her care or payment. Of course, a health plan may make these disclosures as directed under a HIPAA-compliant authorization completed by the individual.

A covered health plan or other covered entity may only disclose the relevant PHI to these persons if the individual does not object or the covered entity can reasonably infer from the circumstances that the individual does not object to the disclosure; however, when the individual is not present or is incapacitated, the covered entity can make the disclosure if, in the exercise of professional judgment, it believes the disclosure is in the best interests of the individual.

The Department of Health and Human Services provides the following examples

A health plan may disclose relevant PHI to a beneficiary's daughter who has called to assist her hospitalized, elderly parent in resolving a claims or other payment issue.

A health plan may disclose relevant PHI to a human resources representative who has called the plan with the beneficiary also on the line, or who could turn the phone over to the beneficiary, who could then confirm that the representative calling is assisting the beneficiary.

A health plan may disclose relevant PHI to a Congressional office or staffer that has faxed to the plan a letter or e-mail it received from the beneficiary requesting intervention with respect to a health care claim, which assures the plan that the beneficiary has requested the Congressional Office's assistance.

A Medicare Part D plan may disclose relevant PHI to a staff person with the Centers for Medicare and Medicaid Services (CMS) who contacts the plan to assist an individual regarding the Part D benefit, if the information offered by the CMS staff person about the individual and the individual's concerns is sufficient to reasonably satisfy the plan that the individual has requested the CMS staff person's assistance.

In response to this guidance, covered health plans and other covered entities should review their current policies and procedures to determine what practice works best for them. After such a review the preferred practice may be to require authorizations in these situations. Additionally, even if a disclosure would be permitted under the HIPAA Privacy Rule, many insurance companies and third party administrators have taken a more stringent view of the regulations, apparently in the abundance of caution; e.g., requiring an authorization where it is not otherwise required. (www.hhs.gov/ocr/hipaa)

PUBLISHED BY:

WALDTHAUSEN & ASSOCIATES, INC., 1910 ABBOTT STREET, SUITE 201, CHARLOTTE, NC 28203, T: 704-372-2172

FIND MORE NEWS ON OUR WEBSITE: www.waldthauseninc.com