VSSP
EMPLOYMENT LAW BULLETIN
VOL. III
NO. 1
FEBRUARY 1, 2006

FMLA: HOW TO ANALYZE THE MEDICAL CERTIFICATE FORM

Under the federal Family and Medical Leave Act, employers can require employees to submit a medical certification form certifying their need for FMLA leave. The medical certification form (bureaucratically named "Certification of Health Care Provider Form WH-380") should be a key component of the employer's administration of FMLA leaves for serious health conditions. With it, employers have the right to question and verify FMLA leave usage. But, how should HR professionals analyze the medical certification forms when employees return them?

Consider analyzing the certification forms by using the following three questions:

1. Is the certification form complete?
2. Does the complete certification form make sense?
3. Is the complete certification form valid?

Is the certification form complete?

The U.S. Department of Labor is clear: It is the employee's responsibility to submit a complete certification form; it is the employee's responsibility to find a health care provider who will provide a complete certification form.

If the form is not complete, then the employer should tell the employee that the form is incomplete and explain what is missing. Then, the employer must give the employee a reasonable opportunity to submit a complete form.

Does the complete form make sense?

Is the form internally consistent? For example, if the doctor checks the box certifying the condition as "chronic" but the medical facts section states "flu," then the form does not make sense.

Under such a scenario, the employer cannot request additional information from the employee's health care provider. However, a heath care provider representing the employer may contact the employee's health care provider, with the employee's permission, to get clarification and confirm authenticity of the certification form.

Alternatively, as discussed below, the employer can require a second opinion.

Is the complete certification form valid?

Are the medical facts consistent with the leave time authorized by the doctor? Do the medical facts indicate a serious health condition?

If the employer has such questions, then the employer should consider requiring a second opinion. With the second opinion, the employer chooses the health care provider. The employer, however, cannot choose a health care provider that it regularly uses. The employer must pay for the second opinion and reimburse the employee's expenses.

If the second opinion disagrees with the first, then the employer may require the employee to get a third opinion, which is final and binding. The third opinion is also at the employer's expense.

Administering FMLA leaves is not a simple task. The three questions can provide a framework for analyzing a key component of the FMLA leave process -- the medical certification form.

By: Allen S. Kinzer • phone: 614.464.8318 • e-mail: askinzer@vssp.com

CAN AN EMPLOYER BE LIABLE FOR FAILING TO INVESTIGATE AN EMPLOYEE'S USE OF A COMPUTER TO ACCESS PORNOGRAPHY?

An employer generally has the right to monitor an employee's use of the internet and e-mail at work as long as it has taken sufficient steps to ensure it has not created an expectation of privacy in its employees with regard to such computer use. However, once an employer avails itself of its right to monitor internet and e-mail use and then discovers illegal or other potentially harmful computer misuse, it may have a duty to take adequate steps to investigate thoroughly and stop such misuse.

In *Doe v. XYC Corporation*, a New Jersey appellate court recently held that an employer could be liable for damages caused by an employee's use of a work computer to post child pornography. In *Doe*, the employer learned that an employee was viewing pornographic websites on his work computer. The employer told the employee to stop this behavior, but did not investigate further the complete nature and extent the employee's pornographic viewing, in part because it had conflicting policies as to its right to monitor its employees' internet use. After being instructed to stop, the employee continued to engage in computer misconduct. Eventually, it was discovered that the employee, while using his employer's computer, had been viewing child pornography and, more significantly, had been covertly taking nude photographs of his own 10-year old stepdaughter and posting them on the internet using his work computer.

The employee's stepdaughter sued the employer, seeking to hold it responsible for the actions of the employee. The trial court granted summary judgment in favor of the employer, but the court of appeals reversed the decision. The appellate court found that there was no evidence that the employer had *actual* knowledge that the employee was using his work computer to transmit the photographs of his stepdaughter or *actual* knowledge that the employee had been viewing child pornography at this computer. Nonetheless, the court found that the employer had *implied* knowledge that the employee was viewing child pornography, because the employer *should have known* that the employee was doing so. The court reasoned that, once the employer discovered that the employee was viewing pornography on his work computer, the employer had a duty to investigate the exact nature of the pornographic sites that the employee was viewing. If the company had complied with this duty, it would have discovered the employee's viewing of child pornography and could have taken further steps to stop such misconduct or report the employee to the authorities. The company's failure to investigate thus made it potentially liable for the subsequent harm to the stepdaughter.

Employers who monitor employee e-mail or internet usage should have a regularly distributed computer policy that should include, among other things:

- Notice that employees should not have an expectation of privacy as to anything they create, store, send or receive on company computers; and
- Notice that the employer may monitor and review any material created, stored, sent or received on its computer resources.

Doe is apparently the first decision to impose on employers a duty to investigate the extent of illicit use of the internet and to impose liability for such illicit use. Other courts may not follow the reasoning of the *Doe* court. Nonetheless, it may be prudent for employers who discover computer misconduct by an employee to investigate completely and take the necessary steps to stop such misconduct. The case also highlights the danger of having inconsistent internet use and monitoring policies. If you have any concerns with your computer policies or with your obligations to investigate computer misuse, please contact your VSSP attorney.

By: Douglas R. Matthews • phone: 614.464.5460 • e-mail: drmatthews@vssp.com