



*Constance Gilchrest is the research and compliance specialist for Infinisource, Inc., which provides COBRA, flexible benefits and other administrative services to more than 15,000 employers nationwide. She has more than 14 years of experience with COBRA, and is certified for Flexible Compensation Instruction (CFI) through the Employers Council of Flexible Compensation and CDHC Certified through the National Association of Health Underwriters (NAHU).*

# HIPAA's Interaction With FMLA Medical Certifications

*By Constance Gilchrest*

The importance HIPAA places on protecting personal health information is acknowledged by the U.S. Department of Labor (DOL) in recently finalized changes to the Family and Medical Leave Act (FMLA) regulations. Those rules clarify that the requirements of HIPAA's privacy rules must be satisfied whenever an employee's individually identifiable health information is shared with an employer by a HIPAA-covered health care provider.

Some employers think they are exempt from HIPAA's privacy rules since they are not a covered entity. The term "covered entity" does not include employers that create and sponsor group health plans, but most employers are affected by the privacy and security rules either indirectly or directly as the health plan's "fiduciary" under ERISA. Therefore as a practical matter, employers (as plan sponsors) may be required to comply with HIPAA's privacy and security requirements.

In addition, employers come into contact with employees' medical information, especially in the human resources (HR) arena, for the following:

- workers' compensation claims;
- disability plan claims; and
- employee requests for time off under the FMLA.

While these non-health-plan functions are not covered by HIPAA privacy, to perform them employers may need protected health information (PHI) from health care providers that are. Regarding FMLA requests in particular, DOL's Nov. 17, 2008, final rules (73 Fed. Reg. 67934) specify that communication between employers and the employee's health care provider to clarify FMLA certifications also must comply with HIPAA's privacy rules.

HIPAA prohibits a health care provider from disclosing PHI to the patient's employer to verify an FMLA claim, unless the patient has signed a written authorization that complies with HIPAA. The reason employers need an authorization to get an FMLA certification from an employee's health care provider is that the provider is covered by HIPAA, not the employer.

Under the FMLA rules, the employer representative contacting the employee's health care provider must be either a health care practitioner, an HR professional, a leave administrator or a management official. In no case may the employer representative be the employee's direct supervisor. Therefore, to become and remain compliant, employers should have a proper procedure in place to comply with this requirement.

In order to determine what medical information is to be treated as PHI under HIPAA, one should focus on the basis for obtaining the information rather than the nature of the information. Information received by an employer is generally not considered PHI. For example, if an employee submits medical records for the purpose of FMLA certification, the records are employment records, not PHI.

The HIPAA regulations do not hinder the disclosure of PHI for FMLA reasons if the employee has the health care provider complete the medical certification form or document containing the information and requests a copy of that form to take or mail to the employer.

## **Direct Contact With Provider**

However, HIPAA rules do come into play if the employee asks the health care provider to send the completed certification form or other medical information directly to their employer. In this case, the health care provider

**See *FMLA Certifications*, p. 5**

**We've done some remodeling! Check out the new look and features of [thompson.com](http://thompson.com) today!**

## **FMLA Certifications** (continued from page 4)

must receive an authorization form from the employee before sending the information to the employer. In fact, some doctors have refused to complete the FMLA form on the grounds that HIPAA prohibits disclosure of PHI to a third party such as an employer without written authorization.

The FMLA regulations also make it clear that to the extent clarifying the certification requires a HIPAA-covered health care provider to share individually identifiable health information with an employer, HIPAA's privacy rules require a valid HIPAA authorization.

To be valid under HIPAA, the authorization must be a written document containing the following (see ¶410 of the *Guide*):

- the health care provider's name;
- a description of the information to be disclosed;
- the name or specific identification of the person to whom the disclosure can be made;
- a description of the requested disclosure's purpose;
- an expiration date or event for the authorization;
- the signature of the individual making the authorization; and
- three required statements regarding:
  - revocation of the authorization;
  - conditioning treatment or payment; and
  - the potential for re-disclosure.

### **Certification Forms**

DOL developed two new medical certification forms, Form WH-380E for the employee and Form WH-380F for the family member. The revised forms expand the set of information that can be requested from what the prior FMLA rules allowed (see January 2009 newsletter). (The FMLA is enforced by DOL's Employment Standards Administration, not the Employee Benefits Security Administration that handles HIPAA portability and ERISA.)

If the medical certification is incomplete, the new rules require the employer to give the employee written notice as to what sections are incomplete and allow the employee seven days to obtain the missing information. The employer can request recertification every six months. These medical certifications should be kept as confidential

medical records and in separate files from the usual personnel files.

Employers are not covered entities under HIPAA. So while the FMLA certification form from the health care provider contains PHI and sending it to the employer requires the employee's preauthorization, once the employer has the information it is *no longer* considered PHI.

Employers may request PHI to carry out their FMLA obligations. When a health care provider and employer start communicating regarding an individual's health condition or treatment, it is considered PHI. For example, a return-to-work exam would contain PHI, but it would no longer be PHI when held by the employer but this is not a HIPAA-covered activity. (The distinction between PHI and "employment records" is discussed in ¶201.)

The old cliché that there are two sides to every story comes into play when juggling HIPAA and FMLA compliance. Employers need to understand the complex rules and obligations of both the privacy safeguards of HIPAA and the leave rights of the FMLA, the two sides to the story of when PHI can be disclosed (see ¶730 for a detailed discussion of HIPAA/FMLA interaction). 🏠

## **'Secured' PHI** (continued from page 2)

HHS should follow the lead of most state laws and require "a significant risk or harm in order to trigger the breach notification requirement," ABC stated. "Otherwise, individuals will receive notifications for even benign 'breaches' of data."

HHS had published the guidance April 27 (74 Fed. Reg. 19006), seeking public comments on both the guidance itself and the broader breach notification rules that ARRA directs the agency to issue by August. (The comment period expired May 21.)

Although the methods specified in this notice will not actually be "required," using them will create what HHS called "the functional equivalent of a safe harbor" from the breach notification requirement if the PHI is improperly used or disclosed. (See App. C for the full text of the guidance.)

### **For More Information**

The full text of ABC's comments is available on the organization's Web site at [http://www.americanbenefitscouncil.com/documents/hit\\_comments052109.pdf](http://www.americanbenefitscouncil.com/documents/hit_comments052109.pdf). 🏠

New! Try *HR 2009: Answers to Your Top 25 Questions* for 30 days. [www.thompson.com/answ](http://www.thompson.com/answ)