# HUMAN RESOURCES LEGAL UPDATE

## 2013 Annual GMA SHRM
## Human Capital Conference

**Alliant Energy Center**
**Madison, Wisconsin**
**May 14, 2012**

**Attorney Jennifer S. Mirus**
**Boardman & Clark LLP**
**One South Pinckney Street, Fourth Floor**
**P.O. Box 927**
**Madison, Wisconsin 53701-0927**
**Direct Telephone: (608) 283-1799**
**jmirus@boardmanclark.com**

## I. NEW FORM I-9

A. On March 7, 2013, the U.S. Citizenship and Immigration Services (USCIS) issued a new and revised Employment Eligibility Verification Form I-9. The new Form replaces all other forms. Beginning May 7, 2013, employers must use the new version of the Form for all new hires and for re-verifying current employees with expiring employment authorization documentation.

B. The new Form I-9 is now nine pages long, including the form, instructions, and the List of Acceptable Documents. The form itself has been reformatted and expanded from one page to two and includes additional data fields. The primary changes to the form include:

1. Section 1 of the I-9, which requires identifying information about the employee, includes new data fields for foreign passport information (where applicable), telephone number and email addresses.

2. The data fields for telephone number and email addresses are optional, and the instructions provide that the Department of Homeland Security may contact employees if it learns there is a potential mismatch between information provided on the I-9 and information in DHS and Social Security Administration records.

3. There are also boxes for a 3-D barcode on both pages of the new Form I-9; however, USCIS has not clarified the purpose for the boxes.

C. The instructions have also been revised and are intended to be clearer to both employees and employers. For example, the instructions provide specific situations when a Social Security card cannot be used as a document to establish employment authorization.

D. Employers should not complete new Forms for existing employees who do not require re-verification. In addition, employers may not demand or request that the employee produce a specific form of documentation from the List of Acceptable Documents included with the I-9 Form.

E. Employers who fail to properly complete and retain I-9 forms are subject to civil fines of up to $1,100 per form and, in some cases, criminal penalties.

## II. RECENT CHANGES TO THE FEDERAL FMLA

A. On February 6, 2013, the Department of Labor (DOL) issued a final rule which amended certain provisions of the FMLA effective March 8, 2013. The DOL website includes a helpful fact sheet and additional information on the new rule, including a side-by-side comparison of the previous rules to the new rules. http://www.dol.gov/whd/fmla/2013rule/comparison.htm

B. There is a new poster that employers should post immediately.

C. Changes to Qualifying Exigency Leave.

1. The new regulations revise the definitions of "military member" and "active duty." An eligible employee may take FMLA leave for qualifying exigencies arising out of the fact that a military member is on active duty or has been notified of an impending call or order to active duty.

    a. Under the new regulations, the term *military member* (previously referred to as a "covered military member") now includes both members of the National Guard and Reserves *and* the Regular Armed Forces.

    b. The term *covered active duty* (previously referred to as "active duty") requires deployment to a foreign country.

2. The new regulations provide that qualifying exigency leave may be taken for "parental care." An eligible employee may now take leave to care for a military member's parent who is incapable of self-care when the care is necessitated by the military member's covered active duty. The "parental care" qualifying exigency covers an employee's request for leave in order to arrange for alternative care for a military member's parent, to provide care on an immediate need basis or to attend meetings with staff at a military member's parent's care facility.

3. The amount of time an eligible employee may take for rest and recuperation under the qualifying exigency leave provisions is expanded from 5 calendar days to a maximum of 15 calendar days.

D. Changes to Military Caregiver Leave.

1. The definition of a "covered servicemember" has been expanded to include "covered veterans who are undergoing medical treatment, recuperation, or therapy for a serious injury or illness." Under the new regulations, a "covered veteran" is defined as an individual who was discharged or released under conditions other than dishonorable at any time during the five years prior to the first date the eligible employee takes FMLA leave to care for the covered veteran. However, the regulations state that the period between October 28, 2009, the date the NDAA was enacted, and March 8, 2013, the effective date of the new regulations, cannot be counted when determining a covered veteran's five-year eligibility period.

2. Under the regulations, the definition of a serious illness or injury now includes both: (1) an illness or injury incurred in the line of duty on active duty in the Armed Forces; or (2) an illness or injury aggravated in the line of duty.

3. Any period of absence due to or necessitated by USERRA-covered military service must be counted in determining an employee's eligibility for FMLA leave.

E. Tracking Increments of Leave. The new rules clarify that an employer must track FMLA using the smallest increment of time used for other leave, subject to a one-hour maximum. An employer may account for FMLA leave in shorter increments than used for other forms of leave. The regulations also state that an employer may not require an employee to take more leave than is necessary.

F. Compliance with GINA. The new rules provide that FMLA documentation covered by the Genetic Information Non-Discrimination Act ("GINA"), e.g., medical certification forms for family members, must comply with the confidentiality requirements of GINA.

## III. SOCIAL MEDIA

A. Legislation Proposed to Prohibit Access to Personal Social Media Accounts.

1. Following several states that have already passed such laws, legislation has been introduced in Wisconsin to prohibit employers from: 1) requesting an employee or applicant to grant access to, allow observation of, or disclose information that allows access to or observation

of the personal Internet account of the employee or applicant; and 2) discharging, expelling, suspending, disciplining, or otherwise penalizing or discriminating against any person for exercising the right to refuse such a request, opposing such a practice, filing a complaint or attempting to enforce that right, or testifying or assisting in any action or proceeding to enforce that right. (The bill also applies to educational institutions and to landlords).

2. The bill, however, would permit an employer to view, access, or use information about an employee or applicant that can be obtained without access information or that is available from the public domain.

3. The bill would also permit an employer to request or require an employee to disclose access information to the employer or in order for the employer to gain access to or operate an electronic communications device paid for in whole or in part by the employer or to gain access to an account or service that is provided by the employer, that the employee obtained by virtue of the employment relationship or that is used for business purposes.

4. The bill would also allow the employer to:

   a. Discharge or discipline an employee for transferring the employer's proprietary or confidential information or financial data to the employee's personal Internet account without the employer's authorization.

   b. Conduct an investigation or require an employee to cooperate in an investigation of any alleged unauthorized transfer of the employer's proprietary or confidential information or financial data to the employee's personal Internet account or of any other alleged employment−related misconduct or violation of the law.

   c. Restrict or prohibit an employee's access to certain Internet sites while using an electronic communications device paid for in whole or in part by the employer or while using the employer's network or other resources.

   d. Monitor, review, or access electronic data that is stored on an electronic communications device paid for in whole or in part by the employer or electronic data that is traveling through or stored on the employer's network.

   e. Comply with a duty to screen employees or applicants for employment prior to hiring or to monitor or retain employee

communications that is established under federal law or by a self−regulatory organization.

5. The bill provides that an employer does not have a duty to search or monitor the activity of any personal Internet account and that an employer is not liable for any failure to request or require access to or observation of a personal Internet account of an employee or applicant.

B. NLRB on Social Media Policies.

1. Under Section 7 the National Labor Relations Act, employees have the right to engage in concerted activities for the purpose of collective bargaining or "other mutual aid or protection." In general, Section 7 of the Act provides employees the right to discuss or act as a group, or to discuss or take action on behalf of a group, to address the terms and conditions of their employment. Employee conduct is "concerted" (and thus protected by law) if it is engaged in by at least one other employee, on behalf of a group of employees, or if one employee is acting alone in the attempt to initiate group action on an issue of terms and conditions of employment. Concerted activity generally involves circumstances in which individual employees seek to initiate or to induce or to prepare for group action or where employees act to bring truly group complaints to management's attention.

2. It is a violation of the Act for employers to take disciplinary action against employees for engaging in concerted activity. In addition, the Act prohibits employers from establishing policies or procedures that would reasonably tend to chill employees in the exercise of their rights under the Act.

3. The National Labor Relations Board has in recent years taken an aggressive stance on issues that implicate Section 7 rights, and in particular, employer restrictions on employee use of social media. The NLRB issued reports that analyze employer policies and restrictions on employee use of social media in August of 2011, January of 2012 and May of 2012. http://www.nlrb.gov/news-outreach/news-releases/acting-general-counsel-releases-report-employer-social-media-policies

4. An NLRB Administrative Law Judge recently found two out of three of a health care employer's computer use policies governing email and electronic media were found overbroad because they could chill employees' Section 7 rights. http://hr.cch.com/eld/UPMC.pdf

a. The employer had a policy that prohibited the use of email for all non-work solicitations. Other non-work use of the email system was not barred. The solicitation/non-solicitation distinction was

found to be lawful because the line drawn on acceptable and prohibited conduct was solicitation and non-solicitation, not activities that implicated Section 7 activities.

b. The employer also had an electronic mail and messaging policy that prohibited certain employee non-work use of email. Non-work email use was allowed under the policy unless it might be "disruptive" or "offensive" or "harmful to morale." These broad terms, without illustrations or further guidance, were broad and vague enough to potentially chill Section 7 activities. Furthermore, the electronic mail and messaging policy banned solicitation that sought to have employees "support any group or organization, unless sanctioned by [the employer's] executive management. By requiring permission from the employer's executive management, the ALJ reasoned that the rule is reasonably interpreted to mean that Section 7 activity is prohibited without prior management permission. Employees wanting to use email for Section 7 purposes were required to disclose this to and seek permission from management, and the chilling effect was unavoidable.

c. Finally, the employer had a policy regarding acceptable use of IT resources which allowed employees de minimum use of the system for personal reasons to the extent such use neither affected the employee's job performance nor prevented other employees from performing their job duties. The policy further prohibited use of the employer's IT, without the employer's prior written consent, to establish websites, social networks or other web-based applications that described any affiliation with the employer, disparaged the employer, or used the employer's logos or other copyrighted material, among other things. The Administrative Law Judge again found these provisions to be overly broad and vague, and reasonably subject to interpretation that would chill protected concerted activity.

## IV. HIPAA

A. Background

1. Published in the January 25, 2013 edition of the *Federal Register*. The Omnibus Rule makes additions and modifications to the HIPAA rules that were already in place, in particular by finalizing a number of the changes that were introduced with the passage of the HITECH Act on February 17, 2009.

2. The fundamental requirements of HIPAA for covered group health plans are still in place.

3. The effective date of the Omnibus Rule is **March 26, 2013**, with a mandatory compliance date of **September 23, 2013** for most changes (possible extensions exist for required modifications to notices of privacy practices and existing business associate agreements).

B. Primary Areas of Concern for Employers and their Group Health Plans

1. Finalized Breach Notification Rule

a. Presumption of Breach. Impermissible use or disclosure of unsecured PHI results in a presumption of a breach, unless the covered entity can demonstrate a low probability that the PHI has been compromised based on a risk assessment that addresses specific factors.

b. Increased Enforcement. The final rule increase the possibility of enforcement action by HHS, as covered entities are required to report breaches to HHS and reporting a breach may trigger a compliance review or investigation.

2. New enforcement landscape, finalizing changes introduced by the HITECH Act

a. Four Tiered Penalty Structure. Applicable penalties based on state of mind associated with the violation: no knowledge, reasonable cause, willful neglect (corrected), willful neglect (not corrected).

b. Increased Enforcement. More required investigations and require penalties in certain circumstances that previously may have resulted in informal resolution.

c. Liability of Actions of Business Associates. Covered entities may be held liable for HIPAA violations of their business associates where their business associates are acting as their agent.

d. Affirmative Defense for Noncompliance. The Omnibus Rule provides an affirmative defense to penalties where a covered entity corrects a violation within 30 days after it is discovered (or should have been discovered using reasonable diligence).

3. Expanded definition of "business associate"

a. Subcontractors. "Subcontractors" of business associates are now considered business associates.

b. Conduits. Clarification of the "conduit" exception — entities that store PHI on behalf of a covered entity are business associates even if they do not access the PHI.

4. Required changes to business associate agreements, including (among other changes) the addition of the following:

a. Security Rule Compliance. A requirement that the business associate comply, where applicable, with the Security Rule with regard to electronic PHI.

b. Report Breaches. A requirement that the business associate report breaches of unsecured PHI to the covered entity.

c. Subcontractors. A requirement that the business associate enter into appropriate business associate agreements with its subcontractors.

d. Privacy Rule Obligations. A requirement that, to the extent the business associate is to carry out any of the covered entity's obligations under the Privacy Rule, the business associate will comply with the requirements of the Privacy Rule that apply to the covered entity in the performance of that obligation.

e. Minimum Necessary. A requirement that the business associate uses and disclosures of PHI are consistent with the covered entity's minimum necessary policies and procedures.

5. Required changes to notices of privacy practices, including (when applicable) the addition of the following:

a. Uses/Disclosures of PHI Requiring Authorization. A statement regarding the necessity of individual authorization for the use or disclosure of psychotherapy notes, the use of PHI for marketing purposes, the sale of PHI, or the use or disclosure of PHI for purposes not described in the notice or privacy practices, as well as a statement regarding how authorization may be revoked.

b. Fundraising. A statement regarding the use of PHI for fundraising purposes and an individual's right to opt out of receiving fundraising communications.

c. Notice of Breach. A statement informing individuals of their right to receive notice of a breach involving their unsecured PHI.

d. Restrictions on Disclosure. A statement regarding an individual's right to restrict certain disclosures of PHI to a health plan where the PHI pertains to health care services not paid for by the plan (e.g., where the individual paid out of pocket).

e. Genetic Information. A statement that the health plan may not use PHI that is genetic information for underwriting purposes.

6. Various other changes, including changes to the rules regarding the PHI of deceased persons; creation of an individual right to an electronic copy of PHI; revisions to the deadlines for responding to requests for access to PHI; the establishment of the right of an individual to restrict disclosures of PHI related to medical care paid for out of pocket; changes to the authorization requirements for providing immunization records to schools; and revisions to the rules regarding the use of PHI for marketing, fundraising, and research.

7. Adoption of GINA rules

a. Impact on Wellness Plans. Among other things, the Omnibus Rule adopts the GINA prohibition on the use of genetic information, which includes family medical history, in providing rebates, discounts, or other incentives related to health insurance premiums; this may have a direct impact on wellness plans (including plans that use health risk assessments), because it prohibits providing incentives that are tied to the collection of family medical history or other genetic information.

b. Increased Risk of Liability. The GINA rules are not new, but the risk of liability is now greater because GINA violations may result in liability under the HIPAA penalty scheme, which is stricter than the penalty scheme under GINA.

## V. FAIR CREDIT REPORTING ACT

A. Responsibility for enforcement of the Fair Credit Reporting Act (FCRA) has moved from the Federal Trade Commission to the new Consumer Financial Protection Bureau. New forms reflecting the new agency's name and where to file complaints have been issued and must be used effective January 1, 2013.