SCHWARTZ HANNUM PC
Guiding Employers & Educators

Labor and Employment Law Update

DECEMBER 2013

IN THIS ISSUE

New HIPAA Regulations Require Immediate Attention

By Hillary J. Massey and Susan E. Schorr

Entities covered by the Health Insurance Portability and Accountability Act ("HIPAA") and their business associates must immediately comply with new regulations concerning the provision of notice in the event of an unauthorized release of certain protected health information ("PHI").

Under the new regulations, which are formally known as the HIPAA Omnibus Rule:

1. HIPAA applies directly to "business associates," such as vendors who contract with healthcare companies;
2. Covered entities and business associates must conduct a four-factor test to determine whether notice of an unauthorized release of certain PHI is required; and
3. Covered entities must update their Notice of Privacy Practices.

Covered entities that have not already updated their policies and practices to comply with the new regulations should make compliance a top priority.

Background

What Is HIPAA?

HIPAA is a federal law that regulates the use and disclosure of PHI. It does so through provisions known as the Privacy Rule, the Security Rule, and the Breach Notification Rule.

The Privacy Rule gives individuals rights over their PHI and sets rules and limits on who can receive such information. Under this rule, covered entities are generally required to take reasonable steps to limit the use or disclosure of PHI *in any format* (*i.e.*, paper or electronic).

The Security Rule requires covered entities to ensure that any *electronic* PHI is secured and protected from unauthorized access or use. Under this rule, covered entities must adopt and implement physical, technical and administrative safeguards to ensure that electronic PHI remains private and secure.

The Breach Notification Rule requires covered entities to notify individuals, the media and/or the Secretary of the United States Department of Health and Human Services ("HHS") in the event of an unauthorized release of "unsecured" PHI. "Unsecured" PHI is PHI that has not been encrypted or destroyed. Thus, the unauthorized disclosure of *encrypted* PHI is not a breach requiring notice under this rule.

Which Entities Are "Covered"?

Covered entities include: (1) health plans; (2) health care clearinghouses; and (3) health care providers that transmit PHI in electronic form in connection with "covered transactions." "Covered transactions" include "the transmission of information between two parties to carry out financial or administrative activities related to health care," such as:

1. Coordination of benefits;
2. Health care claims or equivalent encounter information;
3. Health care payment and remittance advice;
4. Health plan premium payments;
5. Health care claim status;
6. Enrollment or disenrollment in a health plan;
7. Eligibility for a health plan;
8. Referral certification and authorization;
9. First report of injury;
10. Health care attachments; and
11. Health care electronic funds transfers ("EFTs") and remittance advice.

continued on page 8

SCHWARTZ HANNUM PC
Guiding Employers & Educators

EDITORIAL BOARD
Todd A. Newman . . . . *Editor-in-Chief*
Brian D. Carlson . . . . *Editor*

LABOR AND EMPLOYMENT LAW UPDATE DECEMBER 2013

Data Breaches: The Invisible Threat To Our Schools

By William E. Hannum III[1]

If your school's Director of IT told you today that one of your school's talented, creative, and ambitious students hacked into your school's IT network and accessed the database in which your school stores student grades, tuition data and donor information, including financial account numbers, … what would you do?

As more and more independent schools move towards electronic storage of vital student, employee and donor records, we continue to receive reports of data breaches similar to the one described above. Sometimes the hacker is not a student, but a disgruntled former employee, or a stranger who is looking for financial account numbers. Other times, the data breach is not intentional but results from an accidental loss of a laptop or a USB flash drive containing personal information.

Data breaches can have a significant impact on an independent school's relationships with its students, alums, and their families, as well as with faculty, staff and other employees. After a breach, the affected individuals typically experience reduced trust in the institution, given the apparent inability to safeguard sensitive, personal information. While the appropriate response to a data breach depends on the facts of the situation and applicable state and federal laws, below is a broad, step-by-step framework that may help your school prepare for and respond to a data breach.

1. Promptly Notify Your School's Legal Counsel.

As soon as you discover a data breach, it is crucial to notify your school's legal counsel. Among other considerations, the school may be subject to data breach notification requirements that require prompt action to be taken. Your legal counsel should be able to help you and your school's crisis management team comply with any applicable notification requirements and devise a comprehensive strategy for responding to the data breach.

As of the writing of this article, 46 states, as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have enacted laws that require notification in the event of a data breach. Generally, these laws apply only when certain types of information are compromised. For example, Massachusetts law imposes notification obligations when there is a security breach or unauthorized acquisition or use of "personal information," defined as a Massachusetts resident's "first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password…" On the other hand, for example, Missouri law defines "personal information" more broadly, as also including medical information or health insurance information combined with "an individual's first name or first initial and last name."

State data breach notification laws vary in a number of other ways, including who must be notified of a data breach, the information that must be included in the notification, and the types of notification methods that are acceptable. For example, while Missouri law allows "telephonic notice" of a data breach to affected consumers (so long as the notice is provided directly to the consumer), telephonic notice is not sufficient under the Massachusetts data breach law.

Depending on the information compromised in a data breach, your school may also be required to comply with the data breach laws of *other* states. For example, if your school experiences a data breach involving names and Social Security numbers of Massachusetts residents, your school is obligated to comply with the Massachusetts data breach law, *even if the school is located outside of Massachusetts*. Therefore, when assessing your school's notification obligations, it is important to consider (in consultation with your legal counsel) the residencies of *all* affected individuals, and all of the various data breach laws that may be applicable. Since many independent schools draw students from other states, data breaches often require notifications to be sent around the country.

In addition to notification requirements under state laws, other data breach notification requirements may also apply, depending on your school's operations and the types of information compromised. For example, if your school's health center experiences a data breach, and if it is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA"), then you may be required to provide notification in accordance with the federal Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). Additionally, your school may also be a party to contracts that require it to provide notification of breaches to the other contracting parties. For example, if your school's health center treats students from a neighboring school, the contract with that school may require you to notify it of a data breach affecting its students.

Therefore, after experiencing a breach, it is vital that your school promptly strategize

continued on page 3

1 *Will Hannum gratefully acknowledges Arabela Thomas, formerly with Schwartz Hannum, for her assistance in preparing this article. A previous version of this article appeared in the Sept./Oct. 2013* NBOA Net Assets (NBOA). *The Firm is grateful to* NBOA *for its support in publishing this article.*

continued from page 2

Data Breaches: The Invisible Threat To Our Schools

with its legal counsel about the plan for responding to the breach.

2. Quickly Assess The Nature And Scope Of The Breach.

In order to identify any applicable notification requirements, your school must quickly assess the nature and scope of the data breach, including the type(s) of information compromised and the parties affected by the breach. Generally, this requires identifying and examining all of the affected data and devices, as well as interviewing any individuals who may have information about the breach. During this fact-gathering process, your school's legal counsel should provide you with guidance on preserving evidence relating to the breach and documenting the steps taken to contain and investigate the breach.

Legal counsel should also be involved in the fact-gathering, so as to provide protection under the attorney-client privilege, to the greatest extent possible. The nature and scope of the available protection will vary under state law and with the circumstances. However, generally, having an attorney involved will offer some protection, whereas there will be no such protection if an attorney is not involved.

If criminal activity is suspected (*e.g.*, the data breach is apparently the result of a break-in or hacking), then it is often appropriate (even if not expressly required by law) to notify law enforcement officials of the data breach, so that they may guide or lead the investigation process, as well as provide input as to the timing of notification to affected parties. For example, if a student hacks into the school's computer network, law enforcement may be interested in speaking with the student and the student's parents before the school speaks to them or notifies them (and the rest of the school community) about the data breach. Generally, we recommend designating the school's legal counsel or a trusted member of the school's crisis management team as the primary contact for law enforcement and any relevant government agencies. The school should ensure that its designated contact has up-to-date information at all times concerning the school's investigation of, and response to, the data breach.

3. Provide Required Notifications And Be Ready For Questions.

Once your school has assessed the data breach, it should provide all legally required notifications in a timely manner, with the assistance of legal counsel. In addition to notice to the affected individuals, many states' laws also require notification to designated government agencies and consumer reporting agencies. For example, under the North Carolina data breach law, in addition to notifying the affected residents of North Carolina, an independent school that experiences a security breach must notify the Consumer Protection Division of the North Carolina Attorney General's Office. Moreover, if pursuant to the North Carolina data breach law the school provides notification to more than 1,000 people at one time, the school also must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (*e.g.*, Equifax, Experian).

Whenever possible, the affected individuals should first learn of the data breach through the school and not through the media. As your school provides any legally required data breach notifications, it is important to have a clear strategy for addressing questions that are likely to result from the notifications. While, in most cases, schools that experience a data breach are not required to provide free credit monitoring to the affected individuals, doing so may be helpful from a public relations perspective and give your community the sense that your school is committed to doing the right thing.

4. Use The Data Breach As A Learning Opportunity.

Hindsight is 20/20, and thus after your school's response to a data breach has concluded, it is helpful to analyze exactly what went wrong and how the school can improve its policies and procedures to prevent future data breaches. For example, does the school have a written policy regarding data security? Was the policy followed in this particular case? If not, why not? Should an employee who did not follow the school's policy be disciplined? Does the school have an acceptable use policy for its students? Was the policy violated? Should the student who violated it be disciplined? Asking these and other questions may help your school minimize the likelihood of another breach.

Earlier this year, a school experienced a data breach when a faculty member left a USB flash drive containing students' names, social security numbers and other sensitive information in his car. The car was broken into, and the USB flash drive was stolen. After the breach, the school examined its policies and decided not to discipline the employee, because its policies at the time of the breach did not prohibit employees from transporting unencrypted student information on portable devices. As this example suggests, adopting a

After a breach, the affected individuals typically experience reduced trust in the institution, given the apparent inability to safeguard sensitive, personal information.

continued on page 5

Unpaid Internships Pose Hazards For Employers

By Julie A. Galvin[1]

A federal court decision from this past summer serves as a timely reminder that using unpaid interns can be risky to for-profit employers.

In *Glatt v. Fox Searchlight Pictures, Inc.*, a New York federal district court judge determined that two former unpaid interns for a film production company did not fall within the narrow "trainee" exception to the federal Fair Labor Standards Act ("FLSA"). As a result, the court concluded, the interns should have been classified as employees under the FLSA and, as such, could now recover unpaid minimum wages and overtime earnings under this statute, as well as any additional amounts that may be recoverable under the New York wage-and-hour law.

While *Glatt* does not mark a change in this area of the law, the decision underscores how important it is for employers to ensure that unpaid internships comply with the FLSA and any applicable state laws.

Background

Glatt was brought by several former unpaid interns for Fox Searchlight Pictures, Inc., ("Fox Searchlight"). Two of them ("the plaintiffs") performed "back office" tasks related to production of the film *Black Swan*.

Working up to 50 hours per week, the plaintiffs carried out routine administrative tasks, such as making photocopies, organizing filing cabinets, answering phones, making coffee, ordering lunch, running errands, picking up paychecks for co-workers, tracking and reconciling purchase orders and invoices, and watermarking scripts. The plaintiffs did not hold their internships in conjunction with any formal educational programs, nor did they receive any hands-on training related to actual film production.

After their internships had concluded, the plaintiffs filed suit against Fox Searchlight and its parent company under the FLSA and New York law. The plaintiffs eventually moved for summary judgment, asking the court to rule that they did not fall within the "trainee" exception and, accordingly, were entitled to the protections afforded to employees under the FLSA and state law.

Court's Decision

In its decision, the court noted that the FLSA, as interpreted by the Supreme Court, excludes unpaid "trainees" who perform services for their own educational or professional benefit, rather than for the benefit of the employer. (The U.S. Department of Labor ("DOL") also recognizes an exception to the FLSA for individuals who volunteer their time "for religious, charitable, civic, or humanitarian purposes to non-profit organizations.")

The court analyzed several factors that the DOL has identified as relevant to the determination of whether a for-profit employer may treat an intern as an unpaid trainee. According to the DOL, a court should consider whether:

1. The internship, even though it involves the employer's facilities and business activities, is similar to training that would be given in an educational environment;
2. The internship experience is for the benefit of the intern (as opposed to that of the employer);
3. The intern does not displace regular employees but works under the close supervision of existing staff;
4. The employer derives no immediate advantage from the intern's activities, and on occasion, its operations may actually be impeded;
5. The intern is not necessarily entitled to a job at the conclusion of the internship; and
6. The employer and the intern understand that the intern is not entitled to wages for time spent in the internship.

The court found that, considered as a whole, these factors weighed in favor of the plaintiffs' claim that they were required to be treated as employees. Applying the first factor, the court noted that "[w]hile classroom training is not a prerequisite [for unpaid trainee status], internships must provide something beyond on-the-job training that employees receive." In this case, however, the plaintiffs' purely routine work activities involved "nothing approximating the education they would receive in an academic setting or vocational school."

As to the second DOL factor, Fox Searchlight argued that the plaintiffs benefited from their work activities by gaining resume listings, job references, and exposure to the workings of a production back office. The court responded, however, that "those benefits were incidental to working in the office like any other employee and were not the result of internships intentionally structured to benefit them. Resume listings and job references result from any work relationship, paid or unpaid, and are not the academic or vocational training benefits envisioned by this factor." Thus, the court concluded, Fox Searchlight, and not the plaintiffs, primarily benefited from the plaintiffs' work.

The court also found, in relation to the third factor, that the plaintiffs' work had the effect of displacing employees of Fox Searchlight. In this regard, the court observed that while the plaintiffs' work activities were "menial," those activities were nonetheless

continued on page 5

1 *A previous version of this article appeared in* New England In-House (NEIH). *The Firm is grateful to* NEIH *for its support in publishing this article.*

continued from page 4

Unpaid Internships Pose Hazards For Employers

"essential" and, by Fox Searchlight's own admission, would otherwise have been carried out by paid employees.

Along similar lines, in reference to the fourth DOL criterion, the court noted that Fox Searchlight "does not dispute that it obtained an immediate advantage from [the plaintiffs'] work." The court pointed out that the plaintiffs "performed tasks that would have required paid employees," and that "[t]here is no evidence that they ever impeded [other employees'] work at their internships."

Finally, in reference to the last two factors identified by the DOL, the court acknowledged that the plaintiffs understood that they would not be paid for their services, and that there was no evidence that the plaintiffs were entitled (or believed they were entitled) to job offers at the end of their internships. The court concluded, however, that these factors were not sufficient to overcome the other DOL criteria supporting employee status, particularly given the strong public policy embodied in the FLSA against permitting employees to waive their entitlement to wages.

Accordingly, the court concluded that the plaintiffs were employees for purposes of the FLSA and New York law (which the court found coextensive with the FLSA on this issue), thereby entitling them to potential damages under the minimum-wage and overtime provisions of those statutes.

Recommendations For Employers

In light of *Glatt*, there are a number of steps employers should take if they are considering whether to bring unpaid interns into the workplace.

First and foremost, employers should confer with experienced employment counsel to determine whether workers sought to be classified as unpaid interns fall within the trainee exception (or any other exception) to the FLSA.

It is also vital that unpaid internships be structured in accordance with the factors noted by the DOL. For instance, unpaid internships should, to the greatest extent possible, focus on tasks of educational and career value to the interns, and not on routine administrative tasks that employees otherwise would have to perform.

Additionally, an employer should require each unpaid intern to sign an agreement confirming that no wages, compensation or benefits will be provided in connection with the internship and that the intern will not be entitled to a job offer at the conclusion of the internship.

...the decision underscores how important it is for employers to ensure that unpaid internships comply with the FLSA and any applicable state laws.

Employers should also be aware of any applicable state-law requirements for internships. For example, in Massachusetts, a for-profit employer may need to show that an unpaid internship is part of a formal educational program. Misclassifying interns can be particularly costly for Massachusetts employers, in light of the mandatory treble damages and attorneys' fees awarded to prevailing plaintiffs under the Massachusetts Wage Act.

Finally, employers should ensure that any interns who do not both fall within an exception to the FLSA and satisfy any additional conditions that may be required by state law are paid at least the minimum wage, in addition to overtime pay when applicable.

continued from page 3

Data Breaches: The Invisible Threat To Our Schools

comprehensive data security policy can help your school not only minimize the likelihood of a breach, but also respond appropriately if a breach occurs.

Among other things, your school's data security policy should specify security precautions employees must take when accessing, storing and transporting personal information. Additionally, the policy should discuss the school's strategy for protecting personal information that is accessed or stored by the school's third-party service providers. For example, the school may contract with a third party to administer its employees' flexible spending accounts. If the school provides that third-party administrator with personal information regarding its employees, the school may need to include a provision in the contract requiring the administrator to protect such information in accordance with all applicable laws and to notify the school if the security of the information is breached.

In addition to adopting written policies pertaining to data security, it is also helpful for schools to provide employees with regular training about their policies and procedures for protecting personal information and responding to data breaches. Employees should be informed of the potential consequences of their non-compliance with the school's data security policies and procedures, and the potential impact their non-compliance may have on the school's relationships with the school community. Similarly, students should be informed about the acceptable and unacceptable uses of technology and the consequences of violating the school's technology policies and procedures.

As with many areas of compliance, preparation is key to preventing and being ready to respond effectively to data breaches. We encourage schools to work with experienced counsel and IT professionals to update their data security policies and procedures and to prepare for the possibility of responding to a data breach.

NLRB: Employers May Not Require Confidentiality In All Internal Investigations

By Hillary J. Massey

The National Labor Relations Board ("NLRB" or "Board") recently released an Advice Memorandum reiterating the Board's position that an employer may not instruct employees to keep all workplace investigations confidential. Rather, an employer may issue such a directive only if it can show that the circumstances surrounding a particular investigation justify a confidentiality instruction.

Background

Section 7 of the National Labor Relations Act ("NLRA") gives employees (whether unionized or non-unionized) the right to engage in concerted activities for the purpose of mutual aid or protection. Employees' rights under Section 7 include the right to discuss disciplinary investigations involving fellow employees. The Board and courts have long held that an employer violates Section 8(a)(1) of the NLRA if it maintains a work rule that would reasonably chill employees in the exercise of their Section 7 rights.

In its 2012 *Banner Health* decision, the NLRB held that an employer may instruct employees to keep an ongoing investigation confidential only if the employer can demonstrate a legitimate business justification for doing so that outweighs employees' Section 7 rights to discuss the investigation. In this regard, the Board held that an employer may not simply assert that *all* workplace investigations need to be kept confidential. Rather, an employer must show the existence of one or more specific circumstances establishing a need for confidentiality in each *individual* case – *i.e.*, a need to protect witnesses, avoid fabrication of testimony or destruction of evidence, or prevent a cover-up.

Board's Advice Memorandum

The Board's recent Advice Memorandum involved a paper company known as Verso Paper. Verso Paper's written Code of Conduct included the following language prohibiting employees from discussing ongoing investigations:

Verso has a compelling interest in protecting the integrity of its investigations. In every investigation, Verso has a strong desire to protect witnesses from harassment, intimidation and retaliation, to keep evidence from being destroyed, to ensure that testimony is not fabricated, and to prevent a cover-up. To assist Verso in achieving these objectives, we must maintain the investigation and our role in it in strict confidence. If we do not maintain such confidentiality, we may be subject to disciplinary action up to and including immediate termination.

An unfair labor practice charge challenging this policy was filed with an NLRB regional office, which referred the matter to the Board's Division of Advice for guidance as to whether a formal complaint should issue.

In accord with the Board's *Banner Health* decision, the Division of Advice concluded that the final two sentences of Verso Paper's investigation policy were unlawfully overbroad. The Division of Advice stated that "the Employer cannot maintain a blanket rule regarding the confidentiality of employee investigations, but must demonstrate its need for confidentiality on a case-by-case basis," based on the factors identified by the Board in *Banner Health* – *i.e.*, whether witnesses need to be protected, evidence is in danger of being destroyed, testimony is in danger of being fabricated, or there is a need to prevent a cover-up.

Thus, the Division of Advice concluded that the Board should issue a formal complaint against Verso Paper. (The case ultimately settled before a complaint was issued.)

Recommendations For Employers

In light of the Board's Advice Memorandum and *Banner Health* decision, employers are advised to:

- Review their policies and practices concerning workplace investigations, and, in consultation with counsel, revise them as necessary to ensure that the need for employee confidentiality in investigations is assessed on a case-by-case basis;
- Confer with counsel before terminating or otherwise disciplining an employee for violating a confidentiality policy. If the policy is overly broad, the proposed discipline could spark an unfair labor practice charge; and
- Monitor further developments in this area. In particular, it is likely that future Board decisions will help to clarify the circumstances in which the specific factors identified in Banner Health (e.g., a need to protect witnesses) will be found to justify prohibiting employees from discussing an ongoing investigation.

Please contact us if you have any questions regarding the Board's Advice Memorandum or any other issues relating to workplace investigations. We regularly assist employers with labor relations matters, as well as with internal investigations, and we would be happy to assist you.

Supreme Court Clarifies Definition Of "Supervisor" Under Title VII

By Lori Rittman Clark

The United States Supreme Court has resolved a disagreement among lower courts as to the definition of "supervisor" for purposes of harassment claims under Title VII of the Civil Rights Act of 1964 ("Title VII").

In *Vance v. Ball State University,* the Court held that an employee qualifies as a supervisor – meaning that the employer may be held vicariously liable for his or her conduct – only if the employee has the authority to carry out "tangible employment actions" with regard to the victim of the alleged harassment. In particular, the putative supervisor must be empowered to effect "a significant change in employment status, such as hiring, firing, failing to promote, reassignment with significantly different responsibilities, or a decision causing a significant change in benefits."

The restrictive definition adopted by the Court is favorable for employers, since it limits the circumstances under which an employer may be held liable for harassment by an employee.

Background Legal Principles

The term "supervisor" is not used in Title VII. Rather, the Supreme Court has adopted the term as a means of identifying the class of employees whose actions may give rise to certain types of employer liability under the statute.

Specifically, in two decisions issued together in 1998, *Faragher v. City of Boca Raton* and *Burlington Industries, Inc. v. Ellerth,* the Court ruled that whether an employer may be held liable for an employee's harassment turns substantially on whether the harasser is a "supervisor." If the harasser is a supervisor and the harassment results in an adverse "tangible employment action," such as a demotion or termination, then the employer will be held strictly liable for the harassment. If, on the other hand, there was no such "tangible employment action," the employer can avoid liability by demonstrating that it exercised reasonable care to prevent and eliminate harassment and that the plaintiff unreasonably failed to take advantage of those preventive or remedial opportunities. (This is commonly referred to as the *Faragher-Ellerth* affirmative defense.)

By contrast, where the harasser is not a supervisor, but is merely the victim's co-worker, the legal standard under *Faragher* and *Ellerth* differs. In such cases, the employer may be held liable for the co-worker's harassment only if the employer acted negligently in failing to prevent the harassment from taking place.

As the Supreme Court did not define the term "supervisor" in its *Faragher* and *Ellerth* decisions, the federal courts of appeals adopted varying definitions of the term for purposes of Title VII. For example, the First, Seventh and Eighth Circuits held that a Title VII supervisor must have the power to "hire, fire, demote, promote, transfer or discipline" another employee. By contrast, the Second, Fourth and Ninth Circuits held that any employee who has authority to direct and oversee another employee's day-to-day work qualifies as a supervisor for purposes of Title VII.

The *Vance* Case

The *Vance* litigation gave the Supreme Court an opportunity to resolve this split among the federal circuit courts. The plaintiff in *Vance*, Maetta Vance, is an African-American woman who worked as a catering assistant at Ball State University. Vance's direct supervisor was Bill Kimes, general manager of the Banquet and Catering Department.

Vance first complained to the university in 2005 that two co-workers were harassing her. Specifically, Vance alleged that Saundra Davis had threatened her and that Connie McVicker had directed racial epithets toward her. The university investigated Vance's complaints and ultimately gave McVicker a written warning. Because the university was unable to determine what had transpired between Vance and Davis, it counseled both employees regarding their behavior.

Vance continued to complain of alleged harassment by McVicker and Davis throughout 2006 and 2007. Eventually, Vance filed suit in federal court under Title VII against the university, Kimes, Davis and McVicker, claiming, in part, that the university was liable for the hostile environment allegedly created by Davis because Davis had authority to direct Vance's work and thus qualified as a supervisor under Title VII.

Ruling on the university's motion for summary judgment, the district court held that Davis did not qualify as Vance's supervisor because she lacked the authority to "hire, fire, promote, transfer or discipline" Vance. Thus, the court concluded, the university could not be held liable for Davis's alleged harassment of Vance under the *Faragher-Ellerth* standard. The district court further held that the university could not be held liable to Vance on a negligence theory because it had responded reasonably to the alleged incidents of harassment of which it was aware.

On appeal by Vance, the Seventh Circuit Court of Appeals affirmed the district court's decision. Vance then asked the Supreme Court to review the lower courts' holding as to the supervisory issue, which the Court agreed to do.

Supreme Court's Decision

Affirming the lower courts' holding, the Supreme Court concluded that Davis was not Vance's supervisor for purposes of Title VII. The Court held that "the authority to take tangible employment actions is the defining characteristic of a supervisor," and that Davis did not meet this standard. Accordingly, the

continued on page 9

continued from page 1

New HIPAA Regulations Require Immediate Attention

For many entities, it is fairly clear whether or not they are "covered." Some circumstances, however, present a closer question. For example, a company or independent school[1] with a medical provider on staff may or may not be a covered entity. If the staff medical provider treats minor ailments only, without billing a health insurance plan for the treatment, the entity would *not* be a covered entity. If, however, the provider submits claims to insurance companies, the entity is at least a "hybrid" entity, with a portion being "covered." A detailed discussion of covered entity status is beyond the scope of this article, but we would be happy to discuss any questions related to whether or not your entity is "covered."[2]

The New Regulations

The new regulations modify the obligations of covered entities and business associates in several ways. The key changes are discussed below.

Direct Regulation Of Business Associates; Contract Requirement

The Security Rule and certain requirements of the Privacy Rule now directly apply to "business associates" of covered entities. "Business associates" include entities that perform support functions for covered entities and, thus, have access to PHI. Under the new rule, the definition of "business associate" has been expanded to include subcontractors of business associates and any entity that "creates, receives, maintains or transmits" any PHI on behalf of a covered entity.

The new regulations also govern the terms required to be included in business associate agreements, and require business associates to execute written agreements with their subcontractors. All *new* business associate agreements were required to comply with the new regulations by September 23, 2013. However, business associate agreements entered into before January 25, 2013, must be compliant by September 23, 2014, provided that if such agreements are renewed or modified before this date, then they must be compliant upon renewal or modification. HHS has made available on its website a model business associate agreement. The URL is as follows: *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html*.

New Definition Of "Breach"

One of the more salient features of the new regulations is its definition of "breach," the word used to describe when the security of PHI has been compromised by a covered entity or business associate (and/or its related subcontractors).

Under the new regulations, any acquisition, access, use or disclosure of PHI in violation of the Privacy Rule is presumed to be a reportable breach unless the covered entity or business associate conducts a risk assessment and concludes that there is a low probability that PHI has been "compromised." The risk assessment must consider at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

The previous definition of "breach" focused on whether an individual might have been harmed by the unauthorized access (or risk of access) to PHI.

If a breach affects more than 500 people, covered entities must notify the affected individuals, federal regulators and the media. However, earlier this year, HHS announced a settlement for $50,000 with a small non-profit organization in Idaho for a breach involving fewer than 500 people, signaling that organizations of all sizes are being watched by federal regulators and therefore must ensure that they have adequate data security protections in place.

Updates To Privacy Notices

The new regulations require covered entities to update their Notice of Privacy Practices in several ways. For example, they must describe the types of uses and disclosures of PHI that require an authorization and state that the entity is required by law to notify individuals of breaches. HHS's Office of Civil Rights ("OCR") has issued a model privacy notice. Information about the model notice is available on the OCR website *(http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html)*.

Student Immunizations

The new regulations permit covered entities to share proof of student immunization directly with schools without first obtaining written consent from a parent or legal guardian. While *oral* permission from parents or legal guardians (or from students over 18 and emancipated minors) is still required, this change reduces the documentation necessary between families and their health care providers or health care plans. Accordingly, this change should enable schools to more readily obtain any immunization records required by applicable laws.

Recommendations

As a result of these and other changes to HIPAA, we recommend that independent schools and other employers do the following:

- Assess whether their entity is a "covered entity";
- If so, review their HIPAA policies and procedures and revise them as necessary to ensure compliance;

continued on page 9

1 *If a school is a recipient of funds under the Family Educational Rights and Privacy Act ("FERPA"), its student health records are not considered PHI pursuant to HIPAA, but rather are covered by rules applicable to "education records" under FERPA. Most independent elementary and secondary schools do not receive FERPA funding.*

2 *Simply sponsoring a group health plan administered by an outside insurer is usually not sufficient for an employer to become a covered entity under HIPAA as a "health plan." If, however, an employer is both a plan sponsor and a plan administrator, as may be the case with self-insured plans, it may be regulated by HIPAA, with the following caveat: group health plans that have fewer than 50 participants and are self-administered are exempt from the HIPAA rules.*

continued from page 8

New HIPAA Regulations Require Immediate Attention

- Consider implementing policies and procedures requiring the encryption of all portable devices that may contain PHI;
- Train any personnel who handle PHI or vendor contracts on the changes;
- Review and revise Privacy Notices to ensure they reflect required changes;
- Review all vendor relationships to ensure a Business Associate Agreement exists where required;
- Review all existing Business Associate Agreements for compliance with the new regulations; and
- Review and comply with the new requirements for breach notifications.

Please let us know if you have any questions about the new HIPAA regulations, or if you would like assistance with any aspect of compliance.

continued from page 7

Supreme Court Clarifies Definition Of "Supervisor" Under Title VII

Court ruled, the university could not be held liable for Davis's alleged harassment of Vance.

In adopting this test, the Court rejected the position of the Equal Employment Opportunity Commission ("EEOC") that an individual's mere "ability to exercise significant direction over another's daily work" should be sufficient to confer supervisory status. The Court characterized the EEOC's position as "nebulous," "vague," and "a study in ambiguity."

The Supreme Court explained that "an employer may be vicariously liable for an employee's unlawful harassment only when the employer has empowered that employee to take tangible actions against the victim, *i.e.*, to effect a significant change in employment status, such as hiring, firing, failing to promote, reassignment with significantly different responsibilities, or a decision causing a significant change in benefits."

In contrast to the EEOC's "vague" definition of a supervisor, the Court characterized its definition as "easily workable." The Court added that its holding would facilitate resolution of many disputes by allowing the parties to determine at an early stage whether an alleged harasser was a supervisor for purposes of Title VII.

Recommendations For Employers

As a result of the *Vance* decision, we recommend that employers:

- Ensure that their written job descriptions and related documents are clear as to which employees have authority to take "tangible employment actions" and thereby qualify as supervisors for purposes of Title VII. This will assist employers in taking maximum advantage of the Vance decision;
- Maintain their efforts to prevent workplace harassment through training and other preventive programs; and
- Promptly investigate and remedy, as appropriate, all complaints of harassment. In this regard, even after the Vance decision, an employer can be held liable for a hostile work environment created by a non-supervisory employee's harassment if the employer knew or should have known about the harassment and failed to take prompt remedial action.

If you have questions about the Vance *decision or would like guidance in connection with any harassment or discrimination issue, please don't hesitate to contact us.*

SUCCESS STORY:

SHPC Client Prevails In Arbitration Of Union Grievance Over Nurse's Termination

Schwartz Hannum successfully represented a hospital in a labor arbitration involving a registered nurse who was terminated for misconduct. After a six-day hearing, the arbitrator concluded that the nurse's termination was for "just cause" and denied the union's grievance in full.

The nurse was terminated for failing to document the discarding, or "wasting," of controlled substances and then attempting to cover up her misconduct. In denying the grievance, the arbitrator rejected the union's assertions that the nurse had acted in good faith and that the hospital had failed to conduct an adequate investigation. Similarly, the arbitrator dismissed the union's argument that termination was an excessive sanction because the nurse had not been disciplined for misconduct during her nearly 25 years of employment with the hospital. Rather, the arbitrator found that the nurse's actions constituted egregious misconduct justifying her immediate termination.

Todd A. Newman and Brian D. Carlson were the attorneys involved. Mr. Carlson conducted the hearing.

The Firm regularly assists employers with workplace investigations, grievance arbitrations, and related labor and employment matters and would be happy to provide your organization with guidance and assistance.

Small Firms Face Uphill Battle With H-1B Visas

By Julie A. Galvin

Hiring foreign workers can be a difficult process for any company: it is time-consuming and expensive, and there are only a limited number of visa options available. In particular, the most common visa for foreign professional workers, the H-1B visa, is subject to an annual quota, and demand often exceeds the supply.

Unfortunately, for small firms these can be especially daunting hurdles, and thus they need to plan appropriately to maximize their chances of being able to hire foreign nationals as employees.

H-1B Visas

Employers file H-1B visa petitions on behalf of foreign nationals who are employed in specialty occupations that require the application of highly specialized knowledge and completion of a Bachelor's degree or higher in a related field. Examples of such occupations include engineers, physicians, teachers and accountants.

Under the annual cap, only 65,000 new H-1B visas are issued each year. The cap does not apply to H-1B visa transfers or extensions, or to foreign nationals working for certain educational or non-profit research organizations.

In addition, 20,000 further visas are available to foreign nationals who hold advanced degrees from U.S. academic institutions (commonly referred to as "advanced degree H-1B visas").

The H-1B Lottery System

In a typical year, the number of H-1B petitions filed exceeds the annual quota. For instance, this year, within the first five business days of the filing period, U.S. Citizenship and Immigration Services ("USCIS") received approximately 124,000 petitions for the 85,000 visas allotted. In such instances, USCIS holds a lottery to determine randomly which cases will be selected for processing. If a case is not selected, the employer must wait until the following fiscal year to submit a new petition, meaning that the employer may have to wait an *entire year* to fill a desired opening.

Because H-1B visas do not go into effect until October 1 of each year, October 1 is the necessary start date for employees working under new H-1B visas. However, H-1B petitions can be filed beginning April 1, and, in practice, employers generally file their petitions on or near that date, since the annual H-1B lottery (if necessary) is held shortly after April 1. Therefore, obtaining an H-1B visa often requires significant advance planning, as well as some luck.

Issues Affecting Small Firms

Not only do smaller employers have to go head-to-head with larger companies in seeking H-1B visas (for example, in 2011, Microsoft alone filed over 4,000 H-1B petitions), but they also have their own special set of issues caused by the annual quota.

First of all, the *timing* of the H-1B application process can create difficulties for smaller companies. The H-1B lottery system effectively requires that an employer have its H-1B petitions filed by April 1 for an October 1 start date. Many smaller companies, however, may not have the ability to plan this far ahead or the resources or staff needed to hold a position open until October 1. For example, while a large corporation may have enough software engineers on staff to handle its workload until October 1, a small or start-up company that needs to get a project off the ground may not be able to wait until October 1 to hire a new engineer. In such a case, the company may feel compelled to hire a candidate with current U.S. employment authorization, even if that individual is not the company's top choice. Thus, the timing of the H-1B lottery can put smaller employers at a disadvantage.

In addition, H-1B visas can be *expensive*. Usually, USCIS requires three filing fees for initial H-1B visas, which can range from approximately $1,500 to $2,300 per petition. Because of the complexity of the paperwork, employers are well-advised to hire experienced immigration counsel to assist in the process. Under Department of Labor and USCIS rules, the employer is expected to bear the cost of all business-related expenses associated with the H-1B process, including filing fees and attorneys' fees. Smaller companies may not have the budgets to absorb all of these costs.

Further, petitions submitted by newer companies may be subject to a higher level of *scrutiny* than those submitted by more established companies. To confirm that the company and job opportunity are legitimate, USCIS may ask a newer company for a substantial amount of documentation, such as business licenses, articles of incorporation, financial statements, client contracts, photographs and blueprints of the office premises, and even zoning ordinances for the business's location. A start-up company may not yet have all of the required documentation, and even if it does, collecting and submitting the documentation to USCIS in a timely manner may prove burdensome.

Similarly, as part of an anti-fraud initiative, USCIS routinely conducts *unannounced site visits* to H-1B petitioning employers to verify the information in H-1B petitions. The officer who shows up onsite will expect to speak with a company representative about the foreign national worker and the job opportunity. Handling such an unexpected visit by a USCIS officer may prove challenging for a smaller company that lacks a formal human resources department or similar infrastruc-

continued on page 11

continued from page 10

Small Firms Face Uphill Battle With H-1B Visas

ture, unless the designated point person has been trained in advance.

Finally, additional issues arise if a foreign national wishes to start his or her own company in the U.S. and obtain H-1B sponsorship through that company. If the foreign national is the *owner or majority shareholder* of the company, USCIS may question whether a true employer-employee relationship exists, as self-sponsorship for an H-1B is prohibited. The company would then need to furnish documentation showing that the majority shareholder is, in fact, an employee of the company and subject to its supervision and control (such as by the Board of Directors).

Recommendations For Employers

In light of these issues, we recommend that smaller businesses that want to hire foreign nationals under H-1B visas take the following steps:

- Ensure that new H-1B petitions that are subject to the annual quota are submitted for receipt at USCIS on April 1;
- Review staffing, budgets and similar factors to ensure that the company will be able to function effectively until the H-1B beneficiary is permitted to start on October 1;
- Understand the information contained in the H-1B petition and engage experienced counsel to train the company's H-1B "point person" to properly prepare for any visit by USCIS;
- Be prepared to submit appropriate documentation, if requested by USCIS, to verify that the company is a legitimate business operation; and
- If the H-1B beneficiary is an owner or majority shareholder of the petitioning company, be prepared to submit documentation showing how the H-1B beneficiary will be controlled by the company.

Please contact us if you have any questions regarding H-1B visas or any other immigration issue. The Firm regularly assists employers with preparing and processing employment-based visa applications, and we would welcome the opportunity to assist you.

2013 Super Lawyers Announcement

Schwartz Hannum PC is thrilled to announce that Sara Goldsmith Schwartz and William E. Hannum III were selected for inclusion in 2013 Massachusetts Super Lawyers in the area of Employment & Labor Law.

Sara and Will's listings have been published in the November issues of New England *Super Lawyers Magazine* and *Boston* magazine. Massachusetts Super Lawyers were selected following a "Blue Ribbon Panel" review of the results of ballots sent to 37,000 lawyers throughout Massachusetts by Law & Politics. Lawyers were scored based on the number and types of votes received. Only five percent of Massachusetts lawyers were named for inclusion in 2013 Super Lawyers.

Additionally, Schwartz Hannum PC has been listed in the 2013 *Super Lawyers Business Edition,* also published in November of this year.

The Firm is also thrilled to announce that Jaimie A. McKean has been selected for inclusion in 2013 New England Rising Stars in the area of Employment & Labor Law. Jaimie has received recognition as a Super Lawyers Rising Star since 2008.

Jaimie's recognition also has been published in the November issues of New England *Super Lawyers Magazine* and *Boston* magazine. Only two and one-half percent of Massachusetts lawyers were named for inclusion in 2013 Rising Stars. Each year, Massachusetts lawyers are asked to nominate the best up-and-coming attorneys whom they have personally observed "in action." Massachusetts Rising Stars are then evaluated and selected based on twelve indicators of peer recognition and professional achievement.

We are extremely proud of Sara, Will and Jaimie, congratulate them on receiving these well-deserved recognitions, and extend our thanks to the entire Schwartz Hannum team.

Upcoming Seminar For Independent Schools

December 11, 2013
Criminal Records Risk Management: Best Practices For Minimizing School Liability With Fingerprinting, SORI, FCRA And More
9:00 a.m. – 11:30 a.m.

Winter Webinar Schedule

March 4, 2014
Conducting An I-9 Audit: Tips, Traps And Best Practices
12:00 p.m. - 1:30 p.m. (EST)

Winter Webinar Schedule For Independent Schools

January 8, 2014
Legal Adventures And Hot Topics In Independent Schools
12:00 p.m. - 1:30 p.m. (EST)

January 22, 2014
Criminal Records Risk Management: Best Practices For Minimizing School Liability With Fingerprinting, SORI, FCRA And More
12:00 p.m. - 1:30 p.m. (EST)

January 29, 2014
Getting It Write: Drafting Employee Handbooks
12:00 p.m. - 1:30 p.m. (EST)

February 12, 2014
Best Practices For Preventing And Responding To Allegations Of Sex Abuse
12:00 p.m. - 1:30 p.m. (EST)

March 26, 2014
Risk Management Strategies For Off-Campus Trips And Activities
12:00 p.m. - 1:30 p.m. (EST)

March 31, 2014
Getting It Write: Student Handbooks
12:00 p.m. - 1:30 p.m. (EST)

Please see the Firm's website at **www.shpclaw.com** or contact the Firm's Seminar Coordinator, **Kathie Duffy**, at **kduffy@shpclaw.com** or **(978) 623-0900** for more detailed information on these seminars and webinars and/or to register for one or more of these programs.

Schwartz Hannum focuses exclusively on labor and employment counsel and litigation, together with business immigration and education law. The Firm develops innovative strategies that help prevent and resolve workplace issues skillfully and sensibly. As a management-side firm with a national presence, Schwartz Hannum represents hundreds of clients in industries that include financial services, healthcare, hospitality, manufacturing, non-profit, and technology, as well as handling the full spectrum of issues facing educational institutions. Small organizations and Fortune 100 companies alike rely on Schwartz Hannum for thoughtful legal solutions that help achieve their broader goals and objectives.

11 CHESTNUT STREET, ANDOVER, MA 01810
E-MAIL: shpc@shpclaw.com **TEL:** 978.623.0900
www.shpclaw.com