

What Every U.S. Employer Should Know About Workplace Privacy

Part Two of a Two-Part Series

By Lisa J. Sotto and Elisabeth M. McCarthy

Last month's article discussed background screening and Social Security number laws. This month's installment covers the Health Insurance Portability and Accountability Act of 1996; information security; and monitoring employee telephone, e-mail, and Internet use.

HIPAA

Through the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Congress called on the U.S. Department of Health and Human Services ("HHS") to promulgate regulations that would help ensure the privacy and security of health information. The Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") and the Security Standards (the "Security Rule") promulgated pursuant to HIPAA apply to "covered entities" and limit the ability of such entities to use or disclose protected health information ("PHI"). The Privacy Rule defines a "covered entity" as a health plan,

Lisa J. Sotto is a partner in the New York office of Hunton & Williams LLP and heads the firm's Privacy and Information Management Practice. She also serves as Acting Chair of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee. **Elisabeth M. McCarthy** is counsel in the New York office of Hunton & Williams LLP and advises clients on privacy and information management issues.

health care clearinghouse, or health care provider who transmits health information in electronic form in connection with certain specified transactions. While the Privacy Rule and the Security Rule do not directly apply to employers, the requirements of these rules do apply to ERISA-covered "group health plans" that are sponsored by many employers.

The Privacy Rule prohibits covered entities from disclosing PHI except where disclosure is 1) to the individual who is the subject of the PHI, 2) for treatment, payment, or health care operations as defined in the Privacy Rule, 3) authorized by the individual, or 4) specifically permitted without authorization by the individual. The Privacy Rule requires covered entities to adopt written policies and procedures regarding the use and disclosure of PHI that are designed to comply with the Privacy Rule.

The Security Rule imposes obligations on covered entities to ensure the confidentiality, integrity, and availability of all electronic PHI that the covered entity creates, receives, maintains, or transmits. Pursuant to the Security Rule, a covered entity is required to conduct a risk assessment of the potential risks and vulnerabilities to the confidentiality of electronic PHI held by the covered entity and to implement a risk management program to reduce the identified risks and vulnerabilities to a reasonable and appropriate level. Covered entities must have in place certain specified administrative, physical, and technical safeguards to protect the electronic PHI they maintain. Covered entities are required to adopt written policies and procedures regarding how these adminis-

trative, physical, and technical safeguards will be implemented.

The fundamental purpose of the Privacy Rule and the Security Rule is to preserve and safeguard PHI. Because plan sponsors often perform functions that are integral to the functions of group health plans and thus require access to an individual's health information held by the group health plan, the Privacy Rule restricts the flow of information from the group health plan to the employer plan sponsor. Under the Privacy Rule, a group health plan may disclose PHI to its plan sponsor only for limited purposes and only after the plan sponsor has complied with the Rule's prescribed requirements for disclosure. The principal purpose of this regulatory barrier between a "group health plan" and an employer plan sponsor is to prevent employers from using their employees' PHI to make employment-related decisions. It is worth noting, however, that the Privacy Rule exempts from the definition of PHI, employment records held by a covered entity in its role as employer. Pursuant to this exemption, to the extent that an employer in its capacity other than as plan sponsor collects and maintains health information regarding its employees, HIPAA would not apply.

To determine the impact of the Privacy Rule, an organization must examine 1) the type of health information the plan sponsor receives; 2) the purposes for which the plan sponsor receives information; and 3) the extent, if any, to which the plan sponsor performs administrative functions on behalf of the group health plan.

continued on page 2

Workplace Privacy

continued from page 1

The Privacy Rule defines a plan sponsor's responsibilities based on whether the plan sponsor receives "protected health information" or "summary health information." A plan sponsor that receives summary health information — that is, information that is a subset of PHI that summarizes claims history, expense, or experience and is stripped of certain personal identifiers — is minimally impacted by the Privacy Rule. A plan sponsor that needs only summary health information to effectively manage its health benefits program may receive the information if it agrees to limit its use of the information to 1) obtaining premium bids for providing health insurance coverage to the group health plan, or 2) modifying, amending, or terminating the group health plan.

On the other hand, a plan sponsor that receives PHI is subject to increased operational and administrative burdens. Plan sponsors typically may receive PHI either from the group health plan itself or from another entity (such as an insurer) that administers the company's health benefits program. Before a plan sponsor may receive PHI, the group health plan or the insurer acting on behalf of the plan must get assurance in the form of a "certification" that the plan sponsor has complied with the new regulatory requirements.

A plan sponsor must certify to the group health plan that it has amended the plan documents to incorporate various provisions. Unless disclosing PHI for enrollment purposes, the plan documents need to be amended before the sponsor may receive PHI. The plan sponsor must agree to:

- not use or further disclose PHI except as permitted or required by the plan documents or as required by law;
- ensure that any subcontractors or agents to whom the plan sponsor provides PHI agree to the same restrictions;
- not use or disclose PHI for employment-related actions or in con-

nection with any other benefit or employee benefit plan of the plan sponsor;

- report to the group health plan any use or disclosure that is inconsistent with those provided for in the plan documents;
- allow individuals to inspect and copy PHI about themselves;
- allow individuals to amend PHI about themselves;
- provide individuals with an accounting of disclosures of their PHI;
- make the plan sponsor's practices available to the Department of Health and Human Services ("HHS") for determining compliance;
- return and destroy all PHI when no longer needed, if feasible; and
- ensure that firewalls for records and employees have been established between the group health plan and the plan sponsor.

In addition, the plan documents must identify, either by name or function, any employee of the plan sponsor who receives PHI for payment, health care operations, or other matters related to the group health plan. The plan documents also must restrict access to and use of PHI to specific, identified employees for the purpose of completing the administrative functions the plan sponsor performs for the group health plan. Finally, the plan documents must provide an effective mechanism for resolving issues of improper use of or access to PHI. The health insurance issuer or other group health plan may disclose PHI to the plan sponsor only after it receives the plan sponsor's certification indicating that the plan documents were amended.

Disclosure of PHI in violation of HIPAA can result in steep civil and criminal penalties (up to \$250,000 in fines and 10 years of imprisonment). Consequently, employers who act as plan sponsors must carefully assess their compliance with HIPAA's Privacy Rule and Security Rule.

HIPAA establishes a basic level of protection for health information. State laws relating to the privacy of health information are not pre-empted by HIPAA if they offer more stringent protections. Employers should

consider relevant state laws on a case-by-case basis as specific issues arise.

INFORMATION SECURITY

Security Breach

Notification Laws

The recent increase in identity theft crimes (discussed earlier) resulted in the enactment of numerous state security breach notification laws. These laws generally do not distinguish between consumers and employees. Consequently, employers would be required to comply with these laws in the event that unauthorized individuals acquire certain employee personal information. A security breach occurs when an unauthorized person acquires or accesses personal information maintained by a company. It is not a breach when an employee or company agent acquires or accesses the data for company purposes as long as the data is not used or disclosed in an unauthorized manner.

Although these laws differ somewhat, generally an entity that maintains "personal information" about individuals needs to notify those individuals of certain security breaches involving computerized data. Specifically, entities are required to notify those whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person. "Personal information" typically means unencrypted data consisting of a person's first name or first initial and last name, in combination with a Social Security number; a driver's license or ID card number; or an account, credit card, or debit card number along with a password or access code. Entities subject to these laws must notify individuals immediately following discovery of a breach if an unauthorized person may have acquired unencrypted electronic personal information.

To date, 29 states have enacted security breach notification laws. Most of these state laws differ at least to some extent. Employers are well advised to determine whether the state in which they operate has a security breach notification law and

continued on page 3

Workplace Privacy

continued from page 2

to comply with such state's specific requirements in the event of a security breach.

Safeguarding Personal Information

Considering the tremendous cost to businesses that suffer security breaches, employers are well advised to develop and implement a plan to safeguard the personal information that they maintain. Such a plan should be appropriate to the size and complexity of the organization, the nature and scope of its activities, and the sensitivity of the information it maintains. While there are a handful of basic elements listed below that every safeguards plan should address, businesses have the flexibility to implement policies, procedures, and technologies that are appropriate to their unique circumstances.

1) Designate one or more employees to coordinate a safeguards program.

Whether an organization tasks a single employee with coordinating safeguards or spreads the responsibility among a team of employees, someone in the organization needs to be accountable for information security. In deciding who it should be, employers should recognize that information security is fundamentally a management issue, not a technology issue. While information technology can play a significant role in protecting data, effective information security requires a broader focus and should include physical security, employee training and management, and business processes.

In addition, an appropriate safeguards program will almost certainly require the coordination of legal, human resources, information technology, audit, and business functions. The person or team that coordinates the program should have the ability to communicate and work effectively with all of these different groups.

2) Identify and assess the risks to individuals' personal information in each relevant area of the company's operations and evaluate the effectiveness of current safeguards for controlling these risks.

To conduct a risk assessment, an employer will need to identify the information that is being protected and the related risks to that information. In particular, an employer should focus on protecting individuals' personal information in addition to the company's business information and operations. To begin, an employer should identify the personal information that it actually collects, how the employer uses it, where it is stored, to whom it is disclosed, who has access to it for what purposes, and how it will ultimately be disposed. The employer should map these data flows and classify data by sensitivity so security measures can be prioritized.

Next, an employer should consider all the ways that personal information can be compromised. While an employer should obviously consider intrusions by computer hackers, employers should also think about ways that employees, service providers, business partners, or vendors could compromise the security of personal information either intentionally or through carelessness. Employers should take into account risks beyond those associated with information technology and consider business processes as well. It is advisable to have the risk assessment process be conducted by a team that includes both technical and business personnel because of their different perspectives on the likelihood and impact of threats.

Once the risks are identified, a gap analysis is necessary to evaluate where current safeguards are inadequate to address the identified risks. Employers should consider the likelihood that a given risk will occur and the severity of the consequences should it happen. Employers should also consider the effectiveness of the various available security measures and their cost, relative to the harm caused by a compromise.

Employers should recognize the full range of potential costs in the event of a security breach: the cost of investigating a security breach; mitigating and remediating damage to systems, and securing the systems after the breach; lost sales or produc-

tivity caused by the unavailability of systems or data; notifying affected individuals and government agencies, as appropriate; responding to regulator inquiries and enforcement actions; legal fees and costs for the defense of private lawsuits; lost customers; reputational damage; and a possible drop in stock price. The harm caused by a compromise should be defined more broadly than just the resulting financial costs.

3) Design and implement a safeguards program, and regularly monitor and test it.

In designing a safeguards program, employers should consider all areas of operations, such as employee management and training; information systems; and managing system failures, which encompasses prevention, detection and response to attacks, intrusions, and other system failures.

The goal is to create security policies and procedures that are more than mere paper and will actually be followed in day-to-day business operations. Employers should monitor and test each of the elements of their program to reveal whether it is being followed consistently and whether it is operating effectively to manage the risks to personal information that it was designed to address.

4) Select appropriate service providers and contract with them to implement safeguards.

When service providers or other third parties have access to data or information systems, steps should be taken to determine whether they can be trusted not to compromise information security and to ensure that they are contractually required to meet specified safeguards standards.

When conducting due diligence on third-party service providers, employers should review an independent audit of the third party's operations; obtain information about the third party from several references or other reliable sources; require that the third party be certified by a recognized trade association or similar authority; review and evaluate the service provider's information security policies and procedures; and take other appropriate measures to

continued on page 4

Workplace Privacy

continued from page 3

determine the competency and integrity of the party.

Contracts with third parties should specifically address safeguards obligations; a general confidentiality provision is not sufficient. Employers should also require third parties to notify them of significant security incidents (so the employer can determine whether it has any legal obligations to provide notice to individuals of a possible data compromise) and to cooperate in responding to security incidents and investigating data breaches. In addition, an employer may want to ask for the right to audit a third party's safeguards program for compliance with legal and contractual requirements.

5) Evaluate and adjust the safeguards program in light of relevant circumstances, including changes in business arrangements or operations, or the results of testing and monitoring.

Security is an ongoing process, not a static condition. Employers need to evaluate and adjust their safeguards program at regular intervals and respond to results obtained through testing and monitoring the program. A safeguards program also will require changes to keep up with technology, business practice, and personnel. Employers should remain vigilant about new or emerging threats to information security and changes in the legal and regulatory environment.

MONITORING EMPLOYEE TELEPHONE, E-MAIL, AND INTERNET USE

Employers have a legitimate interest in knowing how their employees spend their time at work. Inappropriate e-mail can trigger workplace lawsuits and sexual harassment claims. Cyberslacking and excessive personal telephone calls at work waste employee time, costing employers millions of dollars in lost productivity. Technological advances make it increasingly easy for employers to monitor employees and limit negative behavior. Employers should make certain, however, that they understand their legal rights and

obligations before conducting such monitoring.

TELEPHONE MONITORING The Federal Omnibus Crime, Control and Safe Streets Act of 1968

The Federal Omnibus Crime, Control and Safe Streets Act of 1968 (the "Federal Wiretapping Law") governs the access, use, disclosure, interception, and privacy protections associated with wire communications. The Federal Wiretapping Law prohibits the intentional interception of wire communications such as telephone calls. "Intercept" means the acquisition of the contents of any wire communication through the use of any electronic, mechanical, or other device. There are exceptions under the Federal Wiretapping Law for telephone calls intercepted by wire communications service providers in the ordinary course of business and where there is express or implied consent by one of the parties to the communication. Employers generally are considered to be service providers because the employer typically provides the telephone service being used. Whether or not one of these exceptions applies is determined on a case-by-case basis. For example, the Eighth Circuit in *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992), and the 11th Circuit in *Watkins v. L.M., Berry & Co.*, 704 F.2d 577 (11th Cir. 1983), ruled that implied consent does not exist where an employee is only informed that telephone conversations might be monitored. Implied consent requires a higher standard of awareness that monitoring will take place. The court in *Watkins* also held that personal phone calls may not be intercepted in the ordinary course of business, except to guard against unauthorized activity or to determine that such communications are personal. An employer must discontinue recording or monitoring of any personal communication once it is known that the call is personal. In *Deal v. Spears*, the court held that excessive monitoring without a legitimate business purpose is not permitted.

State Wiretapping Laws

Most states have passed anti-wiretapping laws that regulate the interception and recording of telephone

calls. Most states require at least one person who is a party to the conversation to consent to recording the conversation. Some states, however, require the consent of all parties involved.

Employers wishing to monitor telephone conversations of employees should be aware of, and abide by, the applicable state law prior to engaging in such activity.

E-MAIL MONITORING Federal Electronic Communications Privacy Act of 1986 and the Stored Communications Act

Although primarily drafted to apply to law enforcement authorities, the federal Electronic Communications Privacy Act of 1986 ("ECPA") governs the access, use, disclosure, interception, and privacy protections associated with electronic communications. The ECPA prohibits the intentional interception of electronic communications, including e-mail in transit, but not such communications in storage (*ie*, in an e-mail "In Box"). There is an exception, however, for e-mail intercepted in the ordinary course of business and another exception where there is express or implied consent by at least one party to the communication. The ECPA as initially drafted did not apply to electronic communications in storage. The ECPA eventually was amended by the Stored Communications Act, which governs access to electronic communication in storage. This Act prohibits the intentional unauthorized access to e-mail in storage. Service providers, however, are exempt when accessing stored electronic information. Employers generally are considered to be service providers because the employer typically provides the electronic communications service being used. Therefore, the federal statutes permit employers to monitor employee e-mail.

State E-mail Monitoring Laws

Connecticut and Delaware are the only states that specifically regulate the monitoring of employee e-mail by employers. Both states have enacted statutes that require employers to provide advance notice of any

continued on page 5

Workplace Privacy

continued from page 4

electronic monitoring in the workplace and prohibit monitoring without such notice to employees. There is no case law in either Connecticut or Delaware interpreting or applying the relevant statutes.

Connecticut. Section 31-48d of the Connecticut General Statutes governs an employer's ability to electronically monitor its employees. This law requires employers to conspicuously post a notice concerning the types of electronic monitoring in which the employer may engage. "Electronic monitoring" is broadly defined as "the collection of information on an employer's premises concerning employees' activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectric or photo-optical systems."

There is a limited exception for the investigation of illegal activities. Pursuant to the exception, an employer may conduct monitoring without giving prior written notice when 1) an employer has reasonable grounds to believe an employee is engaged in conduct that violates a law, violates legal rights of the employer or other employees, or creates a hostile workplace environment, and 2) electronic monitoring may produce evidence of such misconduct. Violation of the statute may result in monetary penalties.

Delaware. Delaware law requires employers who monitor employees' Internet access, telephone calls, or electronic mail to provide notice to the employees at hiring or before beginning monitoring. Employers may provide notice either by posting it electronically so an employee sees it at least once each day or by providing a one-time notice in writing, in an electronic record or in another electronic form and having it acknowledged by the employee either in writing or electronically. Unlike the Connecticut law, the Delaware law does not exempt employers from giving notice to employees when the monitoring of e-mail communications

is for purposes of investigating an illegal activity. Similar to Connecticut, violation of the statute may result in monetary penalties.

State Wiretapping Laws

Many states have passed anti-wiretapping laws, similar to the ECPA, which regulate the interception of electronic communications. Most states require the consent of at least one person who is a party to the communications. Some states, however, require the consent of all parties involved.

National Labor Relations Board

Workplaces with unionized labor may be subject to additional restrictions on e-mail monitoring. The National Labor Relations Board ("NLRB") Office of General Counsel published an Advice Decision in 1998 stating that business-only e-mail policies (restricting use of e-mail to business purposes only) were unlawful in situations where computers and computer networks are part of employee "work-areas." The NLRB indicated that such policies would deter protected communication among union members. The NLRB found the prohibition of all personal e-mail to be "overbroad and facially unlawful" in situations where the computers are considered an employee's work area because it banned protected oral solicitation by union members. NLRB rules treat union-related oral solicitation and the distribution of written materials differently. An employer may not prohibit all oral solicitation in the work area, but may limit this communication to non-work hours. In finding that the computer systems were part of employee work areas, communications in the work area could not be completely prohibited or limited to business uses without effectively banning oral solicitation in that work area.

INTERNET MONITORING

Employers have a legitimate interest in monitoring the Internet use of employees. Employers should be aware, however, that if they monitor employee Internet use, the information the employer learns or is on notice of as a result of such monitoring may impose a legal obligation on the employer. In *Doe v. XYZ Corp.*,

877 A.2d 1156 (2005), the New Jersey Appellate Court held that an employer that is on notice that one of its employees is using a workplace computer to access child pornography has a duty to investigate the employee, to report the employee's activities to the proper authorities, and to take effective internal action to stop the continuation of such activities.

COMMON LAW PRIVACY

In circumstances where an employee may not be able to prove a violation of federal or state statutory law, the employer may still be liable for common law invasion of privacy. In the United States, there are four privacy torts: 1) intrusion upon seclusion, 2) false light, 3) appropriation of likeness, and 4) public disclosure of embarrassing private facts. The availability of these tort claims depends on the relevant state law and the specific facts alleged. For example, a constitutional right of privacy exists in California and nine other states. Georgia has a common law right of privacy. New York has neither a constitutional nor a common law right of privacy. Of the four privacy torts, intrusion upon seclusion is probably the most relevant to employers.

The Restatement (Second) of Torts §625B defines the tort of intrusion upon seclusion as the intentional intrusion upon the solitude or seclusion of another or his private affairs or concerns that would be "highly offensive to a reasonable person." To determine whether an intrusion would be offensive to a reasonable person, courts have examined the degree of intrusion, the context, the conduct and circumstances surrounding the intrusion, and the intruder's motives and objectives. The key factor, however, is the expectation of the individual whose privacy allegedly was invaded. An individual would have to show that he had a "reasonable expectation of privacy."

The intrusion upon seclusion tort is relevant in the context of information privacy because employees have used it to make arguments against employer monitoring. It is a difficult claim, however, for employees to

continued on page 6

Workplace Privacy

continued from page 5

successfully assert. The U.S. Supreme Court recognized in *O'Connor v. Ortega*, 480 U.S. 709 (1987), that employers have a legitimate interest in monitoring the workspace of their employees. The only cases in which employees have successfully asserted an intrusion upon seclusion claim involve those in which the employer's surveillance activities were considered "outrageous." For example, in *Hawaii v. Bonnell*, 856 P.2d 1265 (Haw. 1993), an employer set up a video camera in an employee break room used only for non-work purposes. The court held that employees have a subjective expectation of privacy to be free from covert video surveillance in the break room and that their subjective expectation was objectively reasonable because the break room was not a public place or subject to public view or hearing. Several court decisions, such as *Smyth v. Pillsbury Co.*, 914 F.Supp. 97 (E.D. Pa. 1996), and *Bobach v. City of Reno*, 932 F.Supp. 1232 (D. Nev. 1996), have allowed employers to monitor employees' use of company e-mail and the Internet, finding that employees do not have a reasonable expectation of privacy with respect to an e-mail message communicated over an employer's computer system.

Employers should take care that telephone conversations of a personal nature are not monitored once it is apparent that the conversation is not related to the legitimate business purpose that prompted the monitoring. If employers want to monitor or record conversations of sales or service representatives with customers, employee telephones used for such purpose should be marked appropriately and a recorded notice should be given at the beginning of the telephone call notifying the customer that the call is being monitored or tape recorded.

Employers should apply the following guidelines when monitoring employees:

- Monitor only if there is a compelling reason;
- Clearly inform employees on the full scope of monitoring in an employee handbook or e-mail to all employees;
- Use the least intrusive measures available;
- Retain information obtained as a result of monitoring for only the time needed;
- Treat all employees uniformly and apply policies consistently; and
- Determine whether monitoring imposes an obligation to take action.

CONCLUSION

Although there is no omnibus U.S. employee privacy law, employers

face myriad privacy requirements with respect to the management of employee personal information. These requirements apply prior to the commencement of the employment relationship, throughout the employment period, and after the relationship has ended. Employers should use caution in collecting, using, and disclosing employee personal information and should aim to comply with all the legal mandates that impact the use of such information. Employers are well advised to develop and implement comprehensive written information security programs to safeguard employee personal information from misuse or unauthorized acquisition. Employers should also develop and implement written policies and procedures with respect to monitoring the behavior of their employees. Although U.S. legal requirements affecting workplace privacy are complex, employers should respect and protect the privacy rights of their employees.



HUNTON &
WILLIAMS

Hunton & Williams LLP • www.hunton.com