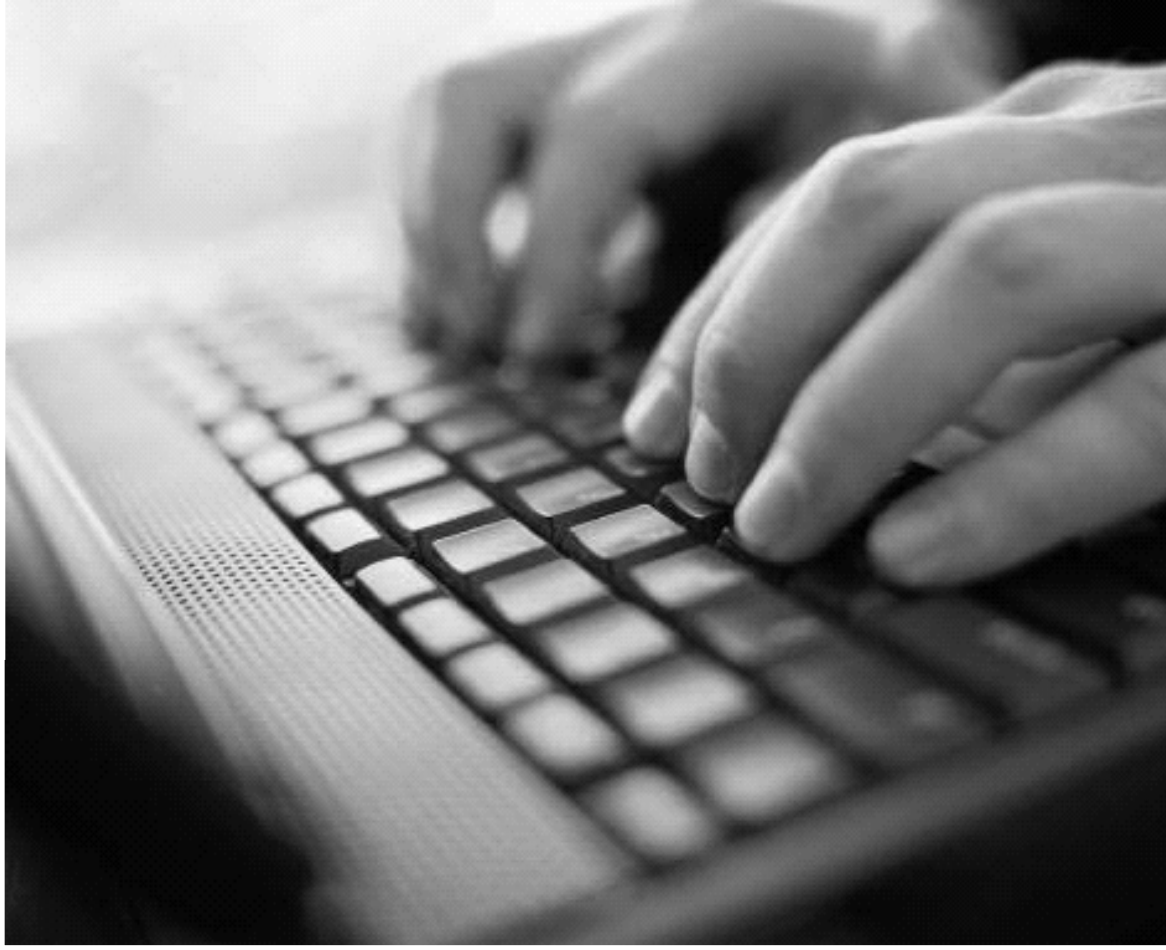

jackson|lewis
Preventive strategies.
Positive solutions.

Data Privacy and Security: A Primer for Law Firms

All We Do Is Work.
Workplace Law. In four time zones and 46 major locations coast to coast.

www.jacksonlewis.com

JACKSON LEWIS

SERVING THE DIVERSE NEEDS OF MANAGEMENT

Jackson Lewis is one of the largest law firms in the country dedicated exclusively to representing management on workplace issues. The Firm has successfully handled cases in every state and is admitted to practice in all Circuit Courts of Appeal and in the United States Supreme Court. With 46 offices and more than 650 attorneys, the Firm has a national perspective and sensitivity to the nuances of regional business environments.

Since 1958 we have represented a wide range of public and private businesses and non-profit institutions in a vast array of industries. When issues arise, we devise optimal solutions that minimize costs and maximize results. Whether we are counseling on legal compliance or litigating a complex case, we assist our clients in achieving their business goals.

In addition, we help employers create policies and procedures promoting positive employee relations. We have built our practice and earned our national reputation over the years by helping companies reduce workplace-related litigation by educating management on legal trends, judicial developments, and statutory and regulatory compliance in the rapidly evolving area of workplace law. Our state-of-the-art preventive law programs utilize the Firm's expertise and unmatched experience to evaluate employment trends and related litigation, minimizing the risk of exposure in future lawsuits.

Data Privacy and Security: A Primer for Law Firms[1]

Law schools in the United States teach their students about a long-standing and fundamental tenet of the legal profession – the attorney-client privilege. It is the general obligation of attorneys to keep client communications confidential. Law schools generally do not teach, at least not nearly to the same degree, how lawyers as law firm business owners ought to protect the personal information of their clients from unauthorized acquisition or access, without hampering their practice. Adopting and implementing safeguards for this purpose is becoming more important for all businesses across the country, particularly for law firms where confidentiality is critical. This primer is intended to provide a brief discussion of the issue and some helpful steps for developing a plan to safeguard such information.

It is difficult to think of areas of practice where a lawyer's work does not involve having some level of access to personal information. Rather, for most areas of practice in the legal profession, in particular medical malpractice litigation, employment law, personal injury and insurance litigation, and family law, attorneys are typically immersed in personal information of their clients and others. No matter how important data privacy and security is to an organization, however, when an attorney is asked about his or her firm's program, a common response is either "the IT Department handles it" or "we have a policy in our handbook" or "our client information is secure," and there typically is no mention of the employees' personal information. Unfortunately, those too often are the wrong responses.

The growing number of data privacy and security laws shows that compliance requires an organization-wide effort to develop written policies and procedures that provide administrative, physical, and technological safeguards for sensitive and personal information. Additionally, the Model Rules of Professional Conduct, specifically Rule 1.6, requires lawyers to "act competently" and protect client information from "inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation … or [under] the lawyer's supervision." These laws and ethical rules do not require protections for confidential firm information or trade secrets, but such information obviously also warrants protection. Leaving this task solely to the firm's IT department will leave the IT employees overwhelmed and the firm overexposed. Law firms also miss the chance at a potential competitive advantage as individuals (clients, employees, others) and business clients increasingly demand heightened privacy and security of their sensitive and personal information.

Some prime examples of the wave of regulation directed at protecting personal information, which could apply to law firms, include:

- **Social Security numbers.** Written policy requirement and other protections for businesses that maintain Social Security numbers in New York, Connecticut, New Jersey, and Michigan;

- **Comprehensive Data Security Program Requirements.** Regulations requiring all businesses adopt comprehensive data privacy and security programs to protect personal information in states such as California, Connecticut, Massachusetts, Nevada, New Jersey (regulations proposed and expected to be finalized soon), Oregon, and Texas;

- **Encryption Mandates.** Data encryption requirements Massachusetts and Nevada;

[1] Prepared by Joseph J. Lazzarotti, Esq., Partner in the Firm's White Plains, NY office.

- **Breach Notification Requirements.** Data breach notification requirements in 46 states and under the Health Information Portability and Accountability Act (for covered entities and business associates, see below);

- **Job Applicant Information.** Specific protections for personal information of job applicants in Utah;

- **"Red Flag" Regulations.** Federal "red flag" regulations for firms that are financial institutions or creditors, although it remains to be seen whether these regulations will ultimately be applicable to law firms since a recent decision by a federal district court held they do not apply to law firms;

- **HIPAA.** Privacy and security requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for company sponsored group health plans (including health flexible spending arrangements) and covered health care providers (including some on-site medical or occupational health clinics). Under recent legislation known as "HITECH", virtually all of these requirements also apply directly to business associates of covered entities, which could include benefits brokers, consultants, third-party administrators, electronic records storage companies and, yes, in some cases law firms. Proposed regulations issued in July 2010 also would apply these requirements to subcontractors of business associates;

- **Federal Contractor Requirements.** Federal contractors generally are subject to the same federal laws, regulations, standards, and policies as the federal agency with which they have contracted. For example, contractors of the Department of Veterans' Affairs must comply with the policies and procedures outlined in VA Directive 6500, *Information Security Program* (http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=50&FType=2).

- **PCI Standards.** Certain firms processing credit card transactions and receiving payment for goods and services through credit cards may need to comply with the Payment Card Industry (PCI) Data Security Standards (https://www.pcisecuritystandards.org/).

- **International Standards.** Firm with subsidiaries or affiliates in other countries such as Canada, France, England or Germany may have difficulties exchanging personal information with their counterparts because of the expansive protections for personal data in those countries. These standards also can complicate the discovery process in this country when important information to be produced resides outside the United States.

In general, these laws and regulations seek to protect certain categories of "personal information." These categories typically include an individual's first name (or first initial) and last name in combination with the individual's (i) Social Security number, (ii) driver's license number, (iii) state identification number, (iv) financial account, debit or credit card number, or (v) health information. Some states have more expansive definitions of personal information. For example, a recent Connecticut statute adds passport numbers, alien registration numbers and health insurance identification numbers to the list. To some degree, all businesses, including law firms, maintain this information in one form or another, about both employees and clients. The protections are far more expansive in other countries.

In the case of HIPAA, for example, law firms representing hospitals, health care providers and health plans often function as business associates. As noted above, under HITECH passed as part of the American

Recovery and Reinvestment Act of 2009 (ARRA), business associates become **directly** subject to certain requirements under the HIPAA privacy and security regulations, including their civil and criminal penalties, in the same manner as those requirements apply to covered entities. This will significantly heighten the obligations of law firms as business associates to safeguard "protected health information" under HIPAA. In addition, as business associates, law firms also are subject to the recent breach notification requirements under HIPAA, which became effective September 23, 2009.

Note also that the laws listed above generally focus on the safeguarding of information and is by no means an exhaustive list of the laws relating to the handling of information by law firms as businesses and as employers. For example, there are rules relating to conducting background checks, monitoring employee emails (including recent developments concerning text messages and personal web-based email accounts of employees), advertising online, and how certain information should be destroyed prior to disposal. Our goal here, again, is to help you begin to chart a path toward adopting and implementing reasonable safeguards for important information maintained by your firm.

So, What Do We Do?

Current data privacy and security laws generally do not contemplate an off-the-shelf policy. Any business, including a law firm, must first assess the risks relating to the sensitive and personal information it possesses by asking questions about how that information is accessed, used, maintained, processed, disclosed, retained, modified and destroyed. At the same time, firms must evaluate the safeguards currently in place. This process, generally referred to as a "risk assessment," is critical to knowing what protections are needed and, in many cases, to learning about the information the firm maintains. Done correctly, the risk assessment process will enable the firm to craft comprehensive policies and procedures to address the risks identified.

Risk assessment. At a minimum, a risk assessment should include:

1. Establishing a key group to coordinate the project, including members of legal, human resources, IT/IS, finance, government relations, marketing, public relations and others.
2. Selecting a project leader and obtain senior management approval early in the process.
3. Formulating a definition of the information to be safeguarded and locating that information. This includes:
    - Identifying all information systems, including all hardware, software and devices such as laptops, blackberries and so on, holding sensitive and personal information.
    - Classifying information, levels of sensitivity.
    - Examining alternative work/business arrangements (e.g., travel and working from home).
    - Determining which employees have access to sensitive and personal information and how the information flows through the organization (e.g., partners, associates, paralegals, internal subject-matter experts, staff, etc.).

- Identifying contractors, vendors and other service providers who maintain sensitive and personal information of the firm or its clients (e.g., expert witnesses, jury consultants, e-discovery providers, etc.)

- Reviewing existing contracts requiring the law firm to safeguard sensitive and personal information.

4. Based on the information collected, identifying applicable laws, e.g., state data security regulations, HIPAA, federal "red flag" regulation, data destruction laws, Social Security number protection laws, e-discovery rules, and so on. A law firm can find itself subject to a number of laws relating to privacy and security of personal information. Consider the following:

    - *Does the firm have a plan for responding to a data breach?* If your state has a breach notification statute, it is very likely that your firm and your clients are subject to it. More companies are experiencing breaches of personal information in their possession, which in many cases require that they notify the affected individuals. Law firms that experience a breach of client personal information likely would be required to notify the firm's client as quickly as possible. The absence of a response plan increases the likelihood of an unnecessary delay and exposure to private lawsuit or state agency action.

    - *Does the firm maintain personal information?* It is hard to imagine a firm that does not have some personal information in its possession. State and/or federal laws likely will apply to most businesses to some degree. For many, this will require that a written security program be adopted and implemented.

    - *Does the firm sponsor or provide services to a health plan or represent a health care provider?* If yes, HIPAA may apply either to the firm's health plan directly and/or to the firm as a business associate. In addition to the obligations described above for business associates, and the breach notification laws in 46 states, the Department of Health and Human Services recently finalized breach notification regulations which require business associates to notify covered entities (e.g., the law firm's clients) of a breach involving unsecured protected health information.

    - *Does the firm maintain medical information about employees in connection with leave determinations and disability accommodations?* If yes, then the information must be segregated, consistent with Family and Medical Leave Act (FMLA) and Americans with Disabilities Act (ADA), and may be subject to the recently enacted Genetic Information Nondiscrimination Act.

    - *Does the firm accept credit cards for payment?* If yes, the firm may need to adhere to the safeguards mandated by the Payment Card Industry Data Security Standards—referred to as PCI DSS.

Developing Safeguards. Once a risk assessment has been conducted, firms need to examine the information they have collected against the safeguards they currently employ to protect it in order to identify vulnerabilities or gaps in those protections. Those vulnerabilities/gaps then must be addressed through additional administrative, physical and technical measures, as appropriate. Examples of safeguards include:

1. Determining whether it is possible to collect, reformat or maintain information in a way that would take it out of the province of data protection laws, or discard it altogether.
2. Limiting access to sensitive and personal information through policy, physical barriers or user profiles, such as using locks on doors and file cabinets, not leaving sensitive and personal information unattended, and using password functions and screensavers.
3. Encrypting portable electronic devices, such as laptops and blackberries, which is required in Massachusetts where technically feasible.
4. Entering into security agreements with vendors holding sensitive and personal information, or taking steps to ensure vendors have adequate safeguards in place.
5. Developing a protocol for responding to data breaches – identify who will lead the response team, prepare template notices, and line up legal counsel and other vendors.
6. Developing a disaster recovery plan.
7. Training staff upon hire and at least annually thereafter, or whenever an event suggests the need for retraining.
8. Developing a record retention policy, maintaining records no longer than is necessary, and destroying information no longer needed.
9. Monitoring legal and technological developments.
10. Evaluating the effectiveness of the data privacy and security program and making changes as appropriate.

Government efforts to regulate the protection of personal information show no sign of slowing. Businesses of all sizes, in all industries, including law, will need to take stock and develop a comprehensive strategy for safeguarding this information. While firms generally should take their size, complexity, capabilities as well as the cost of developing their program into account, the key is to be thorough and thoughtful in identifying and safeguarding the personal information of clients and employees that they maintain.

For additional information, please contact:

Joseph J. Lazzarotti
Jackson Lewis LLP
One North Broadway, 15th Floor
White Plains, NY 10601
(T) 914-514-6107
lazzarottij@jacksonlewis.com

Jason C. Gavejian
Jackson Lewis LLP
220 Headquarters Plaza, East Tower, 7th Floor
Morristown, NJ 07960
(T) 973-538-6890
gavejianj@jacksonlewis.com