DATA PRIVACY AND SECURITY:

A PRIMER FOR LAW FIRMS[1]

Jackson Lewis P.C.

Joseph J. Lazzarotti, Esq., CIPP
Morristown, NJ
(973) 451-6363

Damon W. Silver, Esq.
New York City
(212) 545-4063

www.jacksonlewis.com

While lawyers have long been entrusted with a vast array of confidential and sensitive information, and have long had an ethical obligation to safeguard that information from prying eyes, the challenges of doing so have never been greater. Nor have the risks of legal liability and/or the fatal loss of client confidence. Cyberattacks are projected to cost businesses $2.1 *trillion* a year globally

[1] Prepared by Joseph J. Lazzarotti, Esq., CIPP, Principal in the Firm's Morristown, NJ office, and Damon W. Silver, Esq., Associate in the Firm's New York City office. .

by 2019 and, as a result, businesses are facing enormous pressure from customers, investors, and employees to make data privacy and security a priority – including by carefully scrutinizing the third parties, such as law firms, that they entrust information to. Law firms – which, it is now clear, are preferred targets of cybercriminals[2] – must thus be able to demonstrate to clients that they are prepared to zealously protect their data, and to respond quickly and effectively to cyber events. Firms that cannot will lose business in a hurry.

Beyond client expectations, firms are, in many instances, obligated by law to safeguard certain data. These obligations primarily flow from three areas: statutory and regulatory mandates, contract requirements, and ethical obligations. Compliance with the growing matrix of data privacy and security laws requires a comprehensive effort, which must include the development of written policies and procedures that provide administrative, physical, and technological safeguards for sensitive client and personal information.

Attorneys also have an ethical obligation to safeguard client data; an obligation which is even broader than that required by law, since it applies to *all* client data – not just that which the law protects as personal information. The Model Rules of Professional Conduct, specifically Rule 1.6, require lawyers to "make *reasonable efforts* to prevent the inadvertent or unauthorized disclosure of, or *unauthorized access to*, information relating to the representation of a client." Lawyers are also required to "keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*." *See* Rule 1.1, Comment 8. Additionally, pursuant to Rules 5.1 and 5.3, firms must have policies and procedures in place to ensure staff compliance with the Rules.

Ethics opinions from around the country have discussed the data privacy and security implications of a variety of activities lawyers regularly engage in, such as the use of data storage devices, cloud storage, remote access, and email encryption, as well as issues related to ESI discovery and vendor

[2] To provide a few recent examples, in 2015, Russian cybercriminals attempted to hack the systems of nearly 40 U.S. and UK firms, seeking insider information on which to trade; in May 2016, the International Consortium of Investigative Journalists released a trove of more than 11 million documents that had been stolen by hackers from the boutique Panamanian firm, Mossack Fonseca; and in December 2016, the U.S. Attorney's Office for the S.D.N.Y. charged three Chinese citizens with hacking New York law firms. In announcing the charges, former U.S. Attorney Preet Bhara issued a warning to law firms: "This case of cyber meets securities fraud should serve as a wake-up call for law firms around the world. You are and will be targets of cyber hacking because you have information valuable to would-be criminals." *See also* http://www.jacksonlewis.com/publication/5-practice-tips-law-firms-data-breach-spotlight-swings-their-way.

relationships. The American Bar Association has compiled a helpful chart that tracks these developments nationally.[3]

Given the volume of data firms must safeguard, and the consequences of failing to do so effectively, firms must resist the urge to treat cybersecurity as "the IT Department's problem." An effective cybersecurity program requires participation and buy-in from various departments, including legal, human resources, IT/IS, finance, government relations, marketing, and public relations. Firms that beat their competition to the punch in developing and implementing robust programs will gain an important leg up on their less prepared competitors.

The array of laws and regulations directed at protecting personal information is complex and fast-growing. Some important examples include:

- **Social Security Number Protections.** At least seven states – Connecticut, Massachusetts, Michigan, New Mexico, New Jersey, New York, and Texas – have enacted statutes or regulations obligating businesses to implement policies and procedures to protect the confidentiality and security of the SSNs they maintain. In New York, for example, businesses should have policies in place to limit access to employee SSNs.[4] And, in Michigan and Connecticut,[5] businesses need to maintain and publish specific policies to address the SSNs they acquire.
- **Comprehensive Data Security Program Requirements.** An increasing number of states require businesses to actively safeguard the personal information (*e.g.*, SSNs, drivers' license numbers, financial account numbers (including credit and debit card numbers, and bank account information), medical information, and biometric information) they maintain. These states include California, Connecticut, Florida, Illinois, Indiana, Massachusetts, Maryland, Nevada, New Jersey, Oregon, and Texas. Massachusetts has passed particularly stringent and

[3] https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

[4] N.Y. Gen. Bus. Law §399-dd.

[5] Mich. Comp. Laws § 445.82 *et seq.*; and Conn. Gen. Stat. § Sec. 42-471.

detailed data security regulations[6], as has New York's Department of Financial Services[7]. And in early in 2016, California's Office of the Attorney General issued a report that takes an expansive view of the actions a business must take to "reasonably" protect the data it holds.[8]

- **Encryption Mandates.** Massachusetts and Nevada have both enacted data encryption requirements.
- **Breach Notification Requirements.** Forty-seven states require businesses to provide notice when they experience a "breach" of the "personal information" they maintain. Additionally, firms that provide counsel to health care sector clients may be considered "business associates" under the Health Information Portability and Accountability Act, which has its own breach notification mandates. Notably, a firm's obligations as a business associate do not end with breach notification; they must also adopt and implement comprehensive administrative, physical, and technical safeguards to secure protected health information.
- **PCI Standards.** Firms that process credit card transactions and receive payment for goods and services via credit cards may need to comply with the Payment Card Industry Data Security Standards (PCI-DDS).[9]
- **International Standards.** Firms with subsidiaries, affiliates and clients located in or that conduct business in other countries may have difficulties exchanging personal information with their counterparts, and others, because of the expansive protections for personal data in those countries. These protections can complicate the discovery process when responsive data resides outside the U.S. Firms that transmit data from EU member states to the U.S., for example, will need to join the EU-U.S. Privacy Shield,[10] or to otherwise comply with stringent EU privacy laws.

---

[6] http://www.workplaceprivacyreport.com/2009/11/articles/written-information-security-program/the-final-final-massachusetts-data-security-regulations-and-a-checklist-for-compliance/ (regulatory checklist available)

[7] http://www.jacksonlewis.com/publication/new-york-releases-revised-proposed-cybersecurity-regulations

[8] http://www.workplaceprivacyreport.com/2016/02/articles/data-security/reasonable-data-security-defined-by-california-ag/

[9] https://www.pcisecuritystandards.org

[10] http://www.jacksonlewis.com/publication/eu-us-privacy-shield-qa

The above list, which focuses generally on the safeguarding of personal information, is by no means exhaustive. In fact, there are numerous other areas in which firms may face data-related obligations. These include: background checks, monitoring employee communications (including via company-run email accounts, text messages, and personal web-based email accounts), advertising online, and destroying and disposing of information.

So, What Do We Do?

There are a number of critical steps that businesses, including law firms, need to take to adequately address their cybersecurity risks. Exactly which steps are needed, and the extent of what needs to be done is a function of a number of factors including the nature of the data, the regulatory environment, the amount, manner and frequency with which data is used and disclosed, and, of course, the demand of the client. We do not cover all of these here, instead we briefly summarize two steps all firms would need to take – perform a risk assessment and adopt of appropriate policies and procedures.

Law firms must thoroughly assess the risks to the sensitive and personal information they possess by investigating, among other things, how that information is accessed, used, maintained, processed, disclosed, retained, modified, and destroyed by the firm. This includes thinking through the kinds of threats and vulnerabilities to the data, such as unauthorized access or acquisition, diminished accessibility, or compromised integrity. If the risk assessment is conducted properly, the information gathered and analyzed through that process will position firms to craft comprehensive policies and procedures to address the risks they face. "Off-the-shelf" policies can be helpful but they are unlikely either to address the expansive data privacy and security obligations to which law firms are subject, or to be tailored to the unique practice(s) and operations of the particular firm.

Risk Assessment. At a minimum, the risk assessment process should include:

1. Establishing a key group to coordinate the project, including members of legal, human resources, IT/IS, finance, government relations, marketing, and public relations. (Smaller firms, which may not have clearly defined departments, should identify the persons with responsibilities in these areas, and involve them in the risk assessment process.)

2. Selecting a project leader and obtaining senior management approval early in the process. This is critical for getting the attention of firm personnel and the necessary resources to complete the project.
3. Formulating a definition of protected information (which should include not just personal information, but also client information), and then locating all information that meets that definition. Different classifications of data evaluated for sensitivity.
4. Identifying all information systems, including all hardware, software, and devices (such as laptops, smartphones, and tablets) that hold sensitive and personal information. This includes examining the uses and applicable features of those systems to understand their security strengths and weaknesses.
5. Evaluating how firm employees do their jobs. This includes examining alternative work/business arrangements (*e.g.*, travel and working from home), and determining which employees have access to sensitive client and personal information, and how that information flows through the organization (*e.g.*, to and from partners, associates, paralegals, internal subject-matter experts, and staff).
6. Identifying contractors, vendors, and other service providers who maintain sensitive and personal information of the firm or its clients. Examples include: expert witnesses, e-discovery vendors, cloud service providers, IT support vendors, private investigators, and reprographics service providers. Such third parties, if not carefully vetted and monitored, can expose a firm to significant cybersecurity liability.
7. Reviewing existing client contracts to see what contractual obligations the law firm has agreed to implement to safeguard sensitive client and personal information.
8. Identifying data privacy and security laws the firm is subject to, such as state data security regulations, HIPAA, data destruction laws, and laws mandating protections for Social Security numbers. In evaluating the legal obligations it is subject to, a firm should consider questions such as:

    - *Does it maintain personal information?* Every firm possesses at least some personal formation. As noted above, businesses that possess such information are often required by state and/or federal law to maintain a written information security program to safeguard that information.

- *Does it sponsor or provide services to a health plan or represent a health care provider?* If yes, HIPAA may apply to the firm's health plan directly and/or to the firm in its role as a business associate. As noted above, business associates have a number of detailed data security obligations.
- *Does it 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 and Americans with Disabilities Act regulations, and may be subject to the Genetic Information Nondiscrimination Act. The EEOC has also issued interpretive guidance encouraging businesses to better protect employee medical information.
- *Does it accept credit cards for payment?* If yes, the firm may need to adhere to the safeguards mandated by the PCI-DSS.
- *Does it have a plan for responding to a data breach?* If the firm's state has a breach notification statute, it is very likely that the firm and its clients are subject to it. Businesses are experiencing breaches of personal information with alarming frequency and, in many of these instances, are required to promptly notify affected individuals and government agencies. Firms that experience a breach of a client's personal information will likely be obligated to notify the client as quickly as possible. This is not, of course, a pleasant call for any lawyer to make. However, if the lawyer's firm has a comprehensive plan in place to address such situations, it will be far easier for the firm to avert a client relations disaster. The absence of a well-crafted plan, by contrast, increases the likelihood of unnecessary delays, exposure to private lawsuits and state agency actions, and – consequently – unhappy clients.

Developing Safeguards. After conducting its risk assessment, the firm's next step is to evaluate the adequacy of its administrative, physical, technical and organizational data security safeguards.[11] Examples of key safeguards include:

[11] The Massachusetts Office of Consumer Affairs and Business Regulations has issued a checklist to assist businesses in complying with the State's comprehensive data protection and privacy requirements (*see* 201 C.M.R. 17). While the Massachusetts law applies only to businesses that maintain the "personal information" of State residents, the OCABR

1. Employing policies and procedures to limit the collection, use, and disclosure of information to the minimum extent necessary to service the client.
2. Determining whether it is possible to collect, reformat, or maintain information in a way that removes it from the province of data protection laws.
3. Developing access management policies, and promoting practices, that limit attorney and staff access to personal and sensitive information to only those people for whom, and to those times when, such access is necessary. Firms can achieve this goal through, for example, role-based network access, physical safeguards (such as removing boxes of documents from conference rooms), and using password functions and screensavers.
4. Encrypting portable electronic devices, such as laptops, smartphones, tablets, and remote drives.
5. Entering into security agreements with firm vendors that have access to sensitive client and personal information, and/or taking steps to ensure vendors have adequate safeguards in place.
6. Developing a protocol for responding to data breaches – *e.g.*, identifying who will lead the response team, preparing template notices, lining up legal counsel and other vendors, and practicing the plan through a tabletop exercise.
7. Developing a disaster recovery plan.
8. Training staff upon hire, at least annually thereafter, and whenever an event suggests the need for retraining.
9. Developing a records retention policy that mandates that records be kept no longer than is necessary.
10. Monitoring legal and technological developments.
11. 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. To the contrary, the Trump administration's proposed budget includes $1.5 billion for various cybersecurity efforts, and the New York State Department of Financial Service's new, expansive

---

checklist, which is attached as Exhibit A, lays out many of the issues firms should consider and address when developing their administrative, physical, technical and organizational data security safeguards.

cybersecurity regulations are likely to prompt action by legislators and regulators in other states. Businesses of all sizes, and in all industries – including law – will need to take stock and develop a comprehensive strategy for safeguarding protected information. In developing their cybersecurity programs, law firms generally can and should take into account their size, the relative complexity and sensitivity of the information they maintain, and the costs required to safeguard that information. But no matter their size or area of practice, it is imperative for all firms to ensure that the programs they have in place provide the level of protection that the law – and their clients – demand.

EXHIBIT A

Massachusetts Data Security Compliance Checklist: Minimum "Information Security Program" Requirements	
Requirements for Every Information Security Program	**Status**
In General: ➢ Program must be in writing. ➢ Program must be developed, implemented, maintained and monitored. ➢ Program must have administrative, technical, and physical safeguards and be reasonably consistent with safeguards for protection of personal information and information of a similar character set forth in any applicable state or federal regulations	
Appoint Key Person: Designate one or more employees to maintain the program.	
Risk Assessment: ➢ Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information ➢ Evaluate and improve current safeguards for addressing identified risks through such steps as: o Ongoing employee (including temporary and contract employee) training; o Ensuring employee compliance with policies and procedures; o detecting and preventing security system failures.	
External Employee Access: Develop security policies addressing whether and how employees may keep, access and transport records containing personal information outside of the Company's business premises.	
Discipline: Impose discipline when the Company's program is violated.	
Protocols for Termination of Employment: Establish procedures to immediately terminate access by terminated employees to personal information by physical or electronic access, such as deactivating their passwords and user names, changing locks, retrieving IDs, and so on.	
Oversee Service Providers: A service provider is "any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to the Regulations. To adequately oversee service providers, the Regulations require that covered entities:	

1. Take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with the Regulations and any applicable federal regulations; and 2. Require such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract will be deemed to satisfy this requirement even if the contract does not require the service provider to maintain the appropriate safeguards, **as long as** the contract was entered into no later than March 1, 2010. However, it is recommended that these contracts be amended to include similar provisions as soon as possible, as there may be similar requirements under federal or state law (such as HIPAA or data security laws in Maryland, Oregon or Nevada).	
Physical Access and Storage: Impose reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.	
Monitor Security Program Performance: Establish procedure for regular monitoring to ensure program is operated in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrade information safeguards as necessary.	
Annual Assessment of Scope of Security Program: At least once per year (or whenever there is a material change in business practices that reasonably affects the security or integrity of records containing personal information), reviewing the scope of the program's security measures for adequacy.	
Document Breach Response: Document steps to respond to breach of security and post-breach review of events and actions taken, if any, to make changes in program.	

Additional Requirements if Personal Information is Electronically Stored or Transmitted	Status
The additional elements below apply at a minimum, *and to the extent feasible:* ➢ to every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information, and ➢ be part of a security system established and maintained by such person that covers the person's computers, including any wireless system.	
Implement Secure User Authentication Protocols that: ➢ control user IDs and other identifiers; ➢ reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; ➢ control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; ➢ restrict access to active users/user accounts only; and ➢ block access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.	
Implement Secure Access Control Measures that: ➢ restrict access to personal information to those who need such information to perform their job duties; and ➢ assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.	
Encryption: Encrypt all transmitted records and files containing personal information that will travel across public networks, and transmitted wirelessly.	
Mandatory Encryption for Portable Devices: Encrypt all laptops or other portable devices that store personal information.	
Monitor IT System Use and Access: Perform reasonable monitoring for unauthorized use of or access to personal information.	

Firewall/Malware/Virus Protection: Implement reasonably up-to-date firewall, system security agent software, malware and reasonably up-to-date patches and virus definitions that are reasonably designed to maintain the integrity of the personal information on a system connected to Internet. System also should be designed to receive current security updates on a regular basis.	
Training: Train and educate employees on the proper use of the computer security system and the importance of personal information security.	

4817-0758-7653, v. 2