Protecting Client Information
by Anthony Davis¹ & Michael Downey²

Law firms are entrusted with the most sensitive and valuable information. Lawyers often receive intimate details about their clients’ and others’ personal finances, marriages, criminal histories, and health. Lawyers also receive proprietary information detailing corporate strategies, mergers and acquisitions, inventions, business and even state secrets. The release of such information may be devastating for individual and corporate clients. People may lose their fortunes, their freedom, their reputations, and even – especially where the information relates to witnesses in criminal cases – their lives.

The consequences of an unauthorized or unintended disclosure of client (or law firm) information can be catastrophic for a law firm. In light of state and federal legislation regulating health, financial, and technology secrets, a law firm may face criminal, regulatory, or disciplinary proceedings from an unauthorized release of information. A law firm may also face civil claims, ranging from breach of contract and fiduciary duty to malpractice, defamation or other torts. Law firms may lose loyal clients, or jeopardize the privacy and financial interests of loyal employees. Sometimes, a law firm’s lawyers’ professional liability (LPL) or commercial general insurance (CGL) policies may provide protection, but in many instances, in the absence of separate “cyber” liability coverage, the costs and consequences of unauthorized or unintended disclosures fall full bore upon the firm.

Considering the breadth and magnitude of these risks, as well as the increase in external threats to law firms and their data protection infrastructures, law firms may benefit from examining what information they keep, how they maintain it, and what they would do if (or when) an improper disclosure occurs. In this article, we seek to provide some guidance regarding the data risks that threaten law firms, the obligations law firms have, and what they can do to protect themselves and their information.

Sources of Duties to Protect Information. A lawyer’s duty to protect information generally arises from one (or more) of six sources. These are:

¹ Anthony Davis is a partner in the national lawyer ethics and risk management practice at Hinshaw & Culbertson LLP. Anthony works in the New York office and can be reached at (212) 935-1100 or adavis@hinshawlaw.com.

² Michael Downey is also a partner in the national lawyer ethics and risk management practice at Hinshaw & Culbertson LLP, and a past chair of the ABA Ethics & Technology Committee. Mike works in the St. Louis office and can be reached at (314) 241-2600 or mdowney@hinshawlaw.com.
A fiduciary duty to protect information – particularly client-related or employee-related information – entrusted to the law firm;

A corresponding ethical duty to protect client-related information. Model Rule 1.6, for example, prohibits a lawyer from disclosing “information relating to the representation of a client” unless the client consents, the disclosure is impliedly authorized, or specified exceptional circumstances exist – for example, that the client intends to engage in certain unlawful conduct or someone brings a claim against the lawyer;³

Court-imposed obligations to protect information. Such obligations may arise from court rules, for example a rule protecting confidential information in family law matters, or protective orders entered in particular cases;

Contractual obligations with clients and non-clients, including law firm employees, to protect information.

State or federal statutes regulatory requirements that govern persons who receive or retain certain types of information, such as medical or financial-related information, and state secrets; and

Obligations imposed generally through tort law, such as the obligations to avoid publicizing another’s private information.

These obligations provide a comprehensive web of protection – and of regulation – such that an improper disclosure may violate multiple obligations, and result in severe consequences, regardless of whether the disclosure was intentional or inadvertent. The bedrock principle is client confidentiality, which is the hallmark of the lawyer-client relationship. Law firms must always remain mindful of the fact that the protection of client information is a central element of the services they provide to their clients, as well as a significant obligation they owe to their employees and others.

**Threats to Information.** The threats to all electronically stored information continue to increase. Law firms hold information that could enable anyone who gains unauthorized access to engage misconduct that includes identity theft, insider trading and even blackmail. Not surprisingly, therefore, law firms have become favorite targets of those seeking to obtain and exploit electronically stored information, including (as a 2009 Federal Bureau of Investigations notice warned) computer hackers.

Threats to electronically stored information come from many quarters, and involved varying levels of technological sophistication, from the most rudimentary to the most advanced. Some criminals seek direct access to information that law firms maintain. Others may attack the vessel that holds the information. For instance, a criminal may steal a briefcase, a smart phone, or computer, thereby gaining access to important information stored there. Criminals may also seek to gain access by breaking into an office or hacking into a firm’s computer system.

Criminals are not the only source of threats to law firm information. Disgruntled employees may disclose information in order to harm clients or their law firms, or take information to establish an independent practice, or to help an adversary. And not all threats to the security of

³ See generally ABA Model Rule 1.6.
information are grounded in malice. An employee may lose information, or simply leave it on a
desk, so that an opportunist, perhaps a custodian, may take advantage of information left in
plain sight. Law firms may also be targets for state or corporate spies. Whether an unscrupulous
person or business seeks information for insider trading, to gain a competitive business
advantage or to undermine an adversary’s case, law firms may be prime targets for espionage
efforts.

Just as the sources of risk are numerous, so are the means for obtaining information held by
law firms. The principle threats to information stored by law firms may be divided into three
categories. First is access through electronic means. There is an entire vocabulary for the ways
in which hackers – sometimes called “crackers” – can obtain information. A hacker may use an
iPod to “podslurp” information, or a thumb or flash drive to “thumbsuck” it. Or they may send
an email to “phish” for data or passwords, or tap a Bluetooth device and listen to calls or access
applications by “bluesnarfing.” They may even pose as a “friend” or acquaintance, or at least
use a friendly email or other electronic communication, in the hopes of gaining access to a
computer network, perhaps to review the information or, even worse, to plant spyware – such
as a “Trojan horse” or “bot” – that can provide access and information in the future.

The second type of threat, physical access, is often forgotten, but presents no less danger. The
degree of threat varies widely, from mild, such as reviewing confidential information left in the
open, for example papers left out after business hours on a desk, at a printer or in an unlocked
file cabinet, or where lawyers and staff discuss client matters in public places, or loudly on cell
phones. But physical access may also involve violent conduct, as when a criminal breaks into an
office or locked file cabinet to obtain information. Physical access is also involved when a
disgruntled employee copies files, or when someone decides to engage in dumpster diving
(which, from our experience, occurs significantly more frequently than law firms anticipate).

Third, information may be elicited through “social engineering” or persuasion, the standard tool
of con men, white collar criminals, and corporate spies. Lawyers and staff are often quite willing
to share information about their work and their clients with anyone who shows interest and a
willingness to listen. Law firms often fail to give sufficient importance to whether new
employees, whether lawyers, secretaries, or security guards, are seeking employment with the
hope of accessing and misusing firm information. Corporate spies often thrive on the
information they can obtain through well-placed people, including employees and friendly
conversation.

**Protecting Information.** In light of the variety of threats, and the range of serious negative
consequences that can result from improper disclosure, law firms are at last beginning to take
seriously the need to impose proper protocols in order to protect information in their charge.
At the highest level, some firms have sought to become ISO/IEC27002 compliant and even
certified. ISO/IEC27002 is an information security standard developed by the International
Standards Organization (ISO) and the International Electrotechnical Commission (IEC).
ISO/IEC27002 contains twelve main sections:

1. Risk assessment
2. Security policies
3. Organization of information security
4. Asset management
5. Human resources security  
6. Physical and environmental security  
7. Communications and operations management  
8. Access controls  
9. Information systems acquisition, development, and maintenance  
10. Information security incident management  
11. Business continuity management  
12. Compliance  

Most law firms are not ready to undertake the expenditures of time and money that the full ISO/IEC 27002 certification process requires. In fact, as far as we know, no United States-based firm has received ISO/IEC 27002 certification, although several international firms are now certified. Yet the ISO/IEC 27002 guidelines provide a useful outline for what they may do protect information. Specific protocols for improving data protection include:

Assess where information is located. Conduct an audit to determine what information a law firm holds, where that information resides, and who can obtain access to the information. This assessment should include an audit of the firm’s use of the Internet and remote systems, as well as how paper and electronically stored information is handled throughout its lifecycle (from creation or receipt through disposal).

This assessment should not stop at the function or application level. For example, if a firm is using virtual storage or operating in the cloud, the law firm should obtain information to determine the location and protections that exist for such operations.

Once completed, the assessment should guide the remaining work to improve the protection of confidential information. For example, if a firm determines that it is keeping too much information for too long, or that inappropriate people have access to information, the firm should use that knowledge as it determines what it will keep, where it will store information, and who should have access to that information.

Educate on confidentiality. Law firms should ensure that they educate everyone who has access to information about the value and need for confidentiality, as well as what the firm and individuals can (and are expected to) do to protect information. The goal is to create a “culture of confidentiality”: constituents need to understand that information should not left unnecessarily vulnerable, and should only be shared when necessary or appropriate. This education should reach to all levels of the firm, not just to the lawyers.

Firms should consider establishing and promoting (including through its education program) codes of conduct that include rules on handling client-related and other confidential information. Firms should also use reminders, including on computer log-in screens and the like, to ensure that constituents receive repeated reminders of their need to protect confidentiality.

Firms should also expect to reinforce the education, both in communications and through further training. Law firm constituents also need to know how to raise concerns when they believe data may have been released or data security compromised, and whom to alert when a disclosure is discovered.
Formalize confidentiality. Consider obtaining confidentiality agreements for everyone who has access to information, including employees, non-employees such as custodians, security guards and temporary employees, and providers. Firms should also consider adopting policies and procedures that restrict how information is handled, for example that client documents must be kept on a firm network or in a firm document-management system. Policies establishing confidentiality obligations should express clear penalties for non-compliance, and these should be invoked whenever appropriate.

Adopt physical protections for information. Firms should adopt the physical safeguards necessary to protect confidential information. This will likely include the use of locked or restricted-access areas. It will also include ensuring that adequate facilities are available for the shredding of waste, as well as provisions to ensure that confidential waste is destroyed each day.

Manage electronic information. Many firms have adopted rudimentary policies to protect information, but these may require review and, where appropriate, further enhancement. Most firms do, and all firms need to take steps to ensure that their software – in particular firewalls and anti-virus programs – are current. These protections, as well as systems to ensure the use and updating of adequate passwords, are the minimum in connection with protecting sensitive information. Increasingly, clients themselves are requesting law firms to adopt and use encryption, and firms should not wait for such requests before considering whether, and to what extent to use encryption on some or all of the information they hold. Firms should also review settings on computers, smart phones, and other devices to ensure that these devices do not become the weakest link in a firm’s data protection system.

Firms should consider who has access to and who accesses confidential information. Enterprise rights controls can limit access to those people who actually require access. Does every lawyer and secretary, for example, need access to non-public information relating to a public company’s merger or settlement of a major claim? Firms should also consider monitoring the access to and flow of information, including to determine when unusual amounts of information are moved off the network, so that problems can be detected and promptly addressed. Finally, firms should seriously consider taking the most important confidential information off the network altogether.

Electronic protections often cross-over to include physical protections. Firms may want to adopt a policy that restricts the use of portable electronic data storage and communications systems, particularly around the most sensitive confidential information in their care. Lawyers may consider it odd that a firm would tell them not to bring iPods or cell phones into their offices or into certain work areas, although such rules are quite common at defense contractors or other companies where information security is at a premium. At minimum, firms should seriously consider permitting the use only of firm authorized smart phones that they can wipe clean if lost, and firm-issued, encrypted flash or thumb drives. In addition, if information is saved on individual computers, firms should consider at least requiring the use of encrypted or clean laptops for travel, particularly international travel.

Manage human resources to protecting confidentiality. When hiring, a law firm should appropriately screen employees who will have access to confidential information, including conducting credit and background checks. Having conducted such reviews, firms should make sure that they take adequate steps to address any problems the screening identifies, and to
renew such evaluations on a periodic basis or when circumstances indicate further due diligence is appropriate.

Managing human resources should extend to establishing adequate support systems for employees. These support systems should ensure that people who need help turn to the firm or its support system (such as employee assistance systems), instead of turning against the firm and taking action that may harm the firm or its clients.

Disposal. Particular dangers arise from disposal of law firm-related information. Firms need to ensure they have convenient, adequate receptacles to receive information to be discarded, and that those receptacles are emptied and shredded on a regular basis. Further, firms should make sure that they dispose properly of all electronically stored information, including that they offer secure destruction for home computers or personal equipment that may contain firm-related information. Finally, having assessed what important information they have, firms should clean out (using secure disposal) sensitive information that they no longer require.

Evaluate insurance coverage. As noted at the outset, problems that may arise from inappropriate disclosure of confidential information may fall outside standard lawyers professional liability (LPL) policies. While most larger law firms’ LPL policies may provide some third party coverage related to the loss of client information even the best LPL policy generally does not cover many of the other costs a firm may incur such as notification costs, extra expenses incurred, possible regulatory fines, crisis management costs or loss of profit due to reputational injury.

Insurance can however play an important part in managing the risks of such costs as there are a diverse portfolio of insurance policies available that can protect firms from a broad range of the type of losses that may incur from a release of client information. These so-called “cyber policies” typically provide indemnification for the cost of notice, coverage for fines and damages that may follow a breach of client information security and crisis management costs. More sophisticated policies can also provide extra expense coverage and business interruption and loss of profits coverage.

Prepare for an unauthorized release. Finally, even if firms undertake full-bore efforts to improve their information protection systems, the possibility of an unauthorized or improper release always remains. Firms should prepare for a breach, and how they will respond to a breach, before any breach occurs. The response plan will need to have several components: first, it will likely include a remedial response, for example identifying and closing the system breach. Second, firms may need to provide notice, including to insurers, affected clients, employees, and – particularly under applicable state data protection laws – to regulators. Third, the response plan will also likely include a public relations response to ensure the affected firm’s reputation remains secure with clients and the larger community. Finally, fourth, firms may want to evaluate in advance what action they will take against the breaching party, including possible civil action, such as seeking temporary restraining orders, and, in appropriate circumstances, even criminal prosecution.

Conclusion. The risks that law firms face from improper access to or release of confidential information are best addressed before disclosure occurs. Accordingly, it is vitally important for law firms to assess what information firms have in their custody, how well it is currently
protected, and what enhancements may be needed in order to better protect both their clients’ interests – and their own.