The Sedona Conference Journal

Volume 17 2016

The Sedona Conference Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers

The Sedona Conference

Recommended Citation:

The Sedona Conference, *Commentary on Privacy and Information Security*, 17 SEDONA CONF. J. 1 (2016).

For this and additional publications see:
https://thesedonaconference.org/publications

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complimentary basis to courthouses and public law libraries and by annual subscription to others ($95; $45 for conference participants and Working Group members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference, 301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or info@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC at www.margobdesign.com or mbraman@sedona.net.

Cite items in this volume to "17 Sedona Conf. J. _____ (2016)."

THE SEDONA CONFERENCE COMMENTARY ON PRIVACY AND INFORMATION SECURITY: PRINCIPLES AND GUIDELINES FOR LAWYERS, LAW FIRMS, AND OTHER LEGAL SERVICE PROVIDERS*

A Project of The Sedona Conference Working Group on Electronic Document Retention & Production (WG1)

Author: The Sedona Conference

Editor-in-Chief: David C. Shonka

Team Leader: Gina M. Trimarco

Drafting Team:

John E. Davis
Tara S. Emory
Jenny-Rebecca Lewis
Jeffrey W. McKenna
Kim Baldwin-Stried Reich
James A. Sherer
Joel Wuesthoff

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

PREFACE

Welcome to the final, November 2015, version of The Sedona Conference *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). The Sedona Conference is a 501(c)(3) research and educational institute that exists to allow leading jurists, lawyers, experts, academics, and others, at the cutting edge of issues in the areas of antitrust law, complex litigation, and intellectual property rights, to come together in conferences and mini-think tanks called Working Groups to engage in true dialogue, not debate, in an effort to move the law forward in a reasoned and just way.

The public comment version of The Sedona Conference *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers* was published in July of this year after more than two years of dialogue, review, and revision, including discussion at several working group meetings. After a sixty day public comment period, during which The Sedona Conference sponsored a public webinar on the Commentary, the editors reviewed the comments received as well as the law and made minor revisions in the wording of Principles 1, 2, 4, and 7 to clarify their meaning. Additionally, minor revisions were made to the comments to the Principles, including some paragraph reorganization. I thank all of the drafting team members for their dedication and contribution to this project. Team members that participated and deserve recognition for their work are: John E. Davis, Tara S. Emory, Jenny-Rebecca Lewis, Jeffrey W. McKenna, Kim Baldwin-Stried Reich, James A. Sherer, and Joel Wuesthoff. Finally, The Sedona Conference thanks Gina M. Trimarco for serving as the Team Leader and David C. Shonka for serving as the Editor-in-Chief.

We hope our efforts will be of immediate and practical assistance to judges, parties in litigation and their lawyers, and database management professionals. We continue to welcome comments for consideration in future updates. If you wish to submit feedback, please email us at comments@sedonaconference.org. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Craig Weinlein
Executive Director
The Sedona Conference
November 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Sedona Conference Working Group 1, through its drafting team on Privacy and Information Security, has developed Principles and Guidelines for lawyers, law firms, and other legal service providers. Advances in technology, communications, data storage, and transmission have produced immeasurable societal benefits. However, they have also created unforeseen risks to individual privacy and the security of information that lawyers gather and hold while representing their clients, whether in litigation, in business transactions, or through personal counseling. Personal identities, privacy, confidential client information, work product, and even attorney-client communications have never been more vulnerable to unauthorized disclosures, breaches, loss, or theft than they are today. Yet, the responsibility of all legal service providers to protect such information has not changed. The applicable standards of conduct do not depend on the size or resources of the professional who holds such information.

We recognize, however, that effective privacy and information security does not allow for a one-size-fits-all solution. The nature of the information, the needs of the client, the circumstances in which the information is held, and other factors affect the methods that a reasonably prudent legal service provider should adopt to protect confidential and private information entrusted to its care. In the end, perfect security practices are not required. What is required are well thought-out policies and practices that are both reasonable and appropriate to the circumstances. This Commentary is intended to help all legal service providers—solo practitioners, large law firms, and legal support entities—determine which policies and practices are best suited for each unique situation.

We have divided this Commentary into several discrete sections. Following a brief Introduction and statement of Principles in Section I, Section II identifies some of the major sources of a provider's duty to protect private and confidential information. Section III then describes a process by which legal service providers may conduct thorough security risk assessments, taking into account the information they possess, the vulnerability of that information to unauthorized disclosures, breaches, loss, or theft, and the way in which each provider may mitigate those threats by adopting a structured or layered approach to protect private and confidential information. Finally, Section IV delves into various policies and practices that can address privacy and information security, setting forth processes that can be scaled to the needs and circumstances of an individual legal service provider.

We think the Principles set out in this Commentary provide guidance in protecting private and confidential information. Nonetheless, we recognize that as technology continues to evolve, people will develop new and presently unimagined methods of creating, storing, transmitting, protecting, and even stealing private and confidential information. This of course means that we must all keep Principle 7 below firmly in mind: Legal service providers should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

The principles that inform this Commentary are:

Principle 1: Legal service providers should develop and maintain appropriate knowledge of applicable legal authority including statutes, regulations, rules, and contractual obligations in order to identify, protect, and secure private and confidential information.

Principle 2: Legal service providers should periodically conduct a risk assessment of information within their possession, custody, or control that considers its sensitivity, vulnerability, and the harm that would result from its loss or disclosure.

Principle 3: After completing a risk assessment, legal service providers should develop and implement reasonable and appropriate policies and practices to mitigate the risks identified in the risk assessment.

Principle 4: Legal service providers' policies and practices should address privacy and security in reasonably foreseeable circumstances, and reasonably anticipate the possibility of an unauthorized disclosure, breach, loss, or theft of private or confidential information.

Principle 5: Legal service providers' privacy and information security policies and practices should apply to, and include, regular training for their officers, managers, employees, and relevant contractors.

Principle 6: Legal service providers should monitor their practices for compliance with privacy and security policies.

Principle 7: Legal service providers should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

I. INTRODUCTION AND INFORMATION SECURITY PRINCIPLES

Legal service providers ("LSPs") as well as other professionals[1] rely on communications technology and the rapid, secure sharing of information to conduct business in modern form. The creation and use of electronic information has not only modified business generally, but has also dramatically changed the legal services industry. From the development of international information networks to remote data access and electronic court submissions, technology and law are now integrated, with both positive and negative consequences.

As with all technology, the benefits of an integrated legal practice do not come without new obligations. The new technologies that have transformed the legal industry also threaten privacy, information security, and even the confidentiality of attorney-client communications in ways that were unimaginable a few years ago. This Commentary responds to these challenges with a framework for addressing information privacy and security concerns in the legal industry, and recommends basic steps that all LSPs and Third-Party Service Providers

---

1. As used herein, the term "Legal Service Provider" ("LSP" or "provider") includes lawyers, law firms, and any other person or entity directly engaged in providing legal advice and counsel, and the term "Third-Party Service Provider" ("TPSP") includes the other professionals and organizations who play an integral part in the provision of legal services, such as auditors, outside experts, consultants, and eDiscovery service providers. The term "Legal Services Industry" ("LSI") refers to both LSPs and TPSPs.

Also, as used herein, the term "private information" should be understood broadly to include not just personally identifiable information ("PII"), such as names, addresses, account numbers, and so forth, but also any information about a person that can individually identify them. The term "confidential information" should similarly be understood broadly to include any non-public information about a company or a financial interest whether personally identifiable or not. Questions about the relative sensitivity of various types of private and confidential information are not considered in this Commentary.

("TPSPs") should consider to safeguard the private and confidential information they maintain on behalf of their clients, third parties, and their own organization.

Although societal concerns about privacy and information security have been with us since the days of paper, recent developments in information technology have resulted in new government regulations and oversight, particularly in the health care and financial services industries. The legal profession interacts directly with these industries and, accordingly, this Commentary includes Appendices that highlight the regulations to which both the health care and financial services industries are now subject. Ethical rules, statutes, regulations, and the common law all impose duties on lawyers, and less directly, on much of the legal services industry, to safeguard private and confidential information belonging to clients and third parties. Contracts or retainer agreements may also contain requirements about the safekeeping and handling of confidential information. This Commentary provides some additional steps for both prospective and remedial measures that LSPs should consider.[2]

The discussion in this Commentary is informed by the following guiding principles:

---

2. This Commentary does not address the treatment of confidential information that becomes part of the court record during litigation. That subject was thoroughly treated in *The Sedona Guidelines: Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases*, THE SEDONA CONFERENCE (2007), *available at* https://thesedonaconference.org/download-pub/478. Although that publication is not recent, its observations about the use of protective orders and sealing orders to shield confidential information are still valid, including the balancing tests employed in each situation. However, one may argue that the weight given the potential impact of disclosure of sensitive personal information should be updated in light of the public's greater awareness today about the harm that may result from such disclosure.

Principle 1: Legal service providers should develop and maintain appropriate knowledge of applicable legal authority including statutes, regulations, rules, and contractual obligations in order to identify, protect, and secure private and confidential information.

Comment 1a: Clients and, sometimes, third parties entrust LSPs with private and confidential information, often in electronic form. Electronically stored information is often at risk of loss or unauthorized access because it is mobile, may be accessed remotely, is easily copied (and corrupted), and can involve large volumes of data. LSPs should reasonably protect such private and confidential information while it is in their possession, custody, or control through measures that reasonably guard all the channels through which that data may be accessed. In some circumstances, failure to take reasonable and appropriate steps to protect private and confidential information may expose an LSP to claims for breach of an attorney's professional/ethical obligations to maintain confidentiality of information related to the representation or for violation of various statutory, regulatory, contractual, or common law obligations imposed on the LSP or its client.

Comment 1b: Perfect protection of client data is not possible, practical, or required. LSPs must take reasonable and appropriate measures to protect data, considering factors such as the nature of the data, the risk of unauthorized access, requirements imposed by the client, applicable legal rules, and the costs associated with protecting the data.

Comment 1c: LSPs can take reasonable and appropriate steps to protect and secure private and confidential information by understanding applicable requirements for such information. These requirements arise from many sources, including ethical rules, federal and state statutes and regulations, state common

law, foreign laws, court rules, and contractual requirements. Different levels of protection may be required for information based on many factors, such as the sensitivity of the information, where and how it is stored, and the purpose for which data is entrusted to another party.

Principle 2: Legal service providers should periodically conduct a risk assessment of information within their possession, custody, or control that considers its sensitivity, vulnerability, and the harm that would result from its loss or disclosure.

Comment 2a: The policies and practices employed by an LSP to protect client and third-party private and confidential information will reasonably vary based on the technology at issue and the information to be protected. Each LSP should consider developing a security plan tailored to meet the individual needs of the LSP's information practices, including storage locations, employees, work practices, IT infrastructure, and client security policies, to name a few.

Comment 2b: The following steps can help LSPs create a reasonable and adequate security plan:

- Identify and evaluate the sensitivity of the various types of information within the LSP's possession, custody, or control, and the potential harm that would result from unauthorized disclosure, breach, loss, or theft of that information.
- Identify specific threats and vulnerabilities that could result in unauthorized disclosure, breach, loss, theft, alteration, or unavailability.
- Assess the risk of harm posed by each threat or vulnerability.

The LSP should also consider the integrity, level of sensitivity, and accessibility of private and confidential information. The goal is to keep private and confidential information

free from corruption, accessible only to those who need to use it, and readily accessible when needed.

Principle 3: After completing a risk assessment, legal service providers should develop and implement reasonable and appropriate policies and practices to mitigate the risks identified in the risk assessment.

Comment 3a: After completing a risk assessment of the information in its possession, custody, or control, each LSP should develop and implement a scaled and prioritized plan to protect private and confidential information. This plan should factor in and respond to the sensitivity of different types of information. The plan should also respond to the threats and vulnerabilities identified in the risk assessment and minimize the risks that would result in unauthorized disclosures, breaches, loss, or theft. The policies and practices should also reasonably respond to client-created data privacy and security requirements while enabling the LSP to meet its day-to-day business needs.

In this regard, larger LSPs should consider hiring an information security director or officer and put together a committee with representatives from all interested groups to develop the LSP's policies and practices for accessing information security. Larger LSPs may also consider hiring a separate privacy officer to address specific privacy concerns. Smaller LSPs may wish to hire a consultant to address both information security and privacy and assist in creating the LSP's policies and practices in this area. In the end, what may be most important is that there be a senior level person who has oversight over all parts of the entity, has sufficient expertise to know what needs to be done, has the authority to implement and enforce the plan the LSP develops, and who is held accountable for the success or failure of information security.

Comment 3b: Effective information security practices are an entity-wide concern. The policies should be implemented and enforced systematically from the top to the bottom within the organization, across all departments and units, and among all employees and contractors. An otherwise solid policy can be rendered useless if sound practices in one part of an organization are accompanied by lax practices in another part.

Principle 4: Legal service providers' policies and practices should address privacy and security in reasonably foreseeable circumstances, and reasonably anticipate the possibility of an unauthorized disclosure, breach, loss, or theft of private or confidential information.

Comment 4a: Information technology is complex. Reasonable policies and practices should address the privacy and security of information inside and outside the office environment, while stored, in transit, or accessed remotely. Policies should also address how and when information is shared with third parties, such as outside experts, consultants, TPSPs, co-counsel, adversaries, and courts. LSPs may store confidential information on numerous IT platforms, devices, and media in different locations, some of which may be operated by, or accessible to, third parties such as cloud service providers and their personnel. Confidential information is also routinely transmitted between these platforms and devices. The methods for protecting confidential information while in transit and in storage are as diverse as the threats to the security of such information.

Comment 4b: Accordingly, LSPs should design reasonable policies and practices to address privacy and security in relevant contexts. At a minimum, good policies and practices will: (1) limit access to confidential information to those with a bona fide role-based need for access; (2) provide for physical security; (3) implement information access controls (e.g., multiple factor

authentication, attribute-based access control); (4) consider intrusion detection and prevention technologies; (5) employ appropriate use of encryption technologies; (6) provide for secure back-up/disaster recovery; and (7) ensure the prompt disposition of information that is no longer needed (and hence at risk of theft with no offsetting potential benefit). Most important, LSPs should implement good policies and practices regarding the handling of client and third-party private and confidential information.

Comment 4c: The plan should include a clear incident response procedure to address the unauthorized disclosure, breach, loss, or theft of private and confidential information. The incident response program should include procedures for: (1) reporting each incident to a designated person responsible for implementing the LSP's response plan; (2) identifying the source of the breach; (3) undertaking steps to stop the breach; (4) investigating the extent of any loss or compromise of private or confidential information; (5) providing appropriate notice to the client, relevant law enforcement authorities, and insurers, as necessary; and (6) abiding by applicable data breach notification requirements.

Principle 5: Legal service providers' privacy and information security policies and practices should apply to, and include, regular training for their officers, managers, employees, and relevant contractors.

Comment 5a: Human beings are the weakest link in any information, privacy, or security program. Therefore, a well-designed program to protect private and confidential information will contain robust provisions for training in protecting information. Training that is relevant to recipients should focus on the types of information, legal requirements, and threats that apply to the information the recipient handles, including the

common techniques that data thieves use to gain access to information through deception. Experience has shown that the best and most effective training sessions are interactive and involve testing to confirm that the recipient understands the material. Accordingly, LSPs should seek to conduct or sponsor formal training at regular intervals (ideally annually) for all personnel.

Comment 5b: In addition to formal training, LSPs should institute regular reminders, warnings, tips, and updates to personnel, in order to ensure timely dissemination of information about new rules or threats applicable to the information held by the LSP. The best security practices appear to be those in which LSPs foster a culture and environment in which everyone is vigilant and aware of what is required in order to maintain security, both individually and across the organization.

Principle 6: Legal service providers should monitor their practices for compliance with privacy and security policies.

Comment 6a: Security breaches can come from many sources, internal or external. The cause may be intentional, negligent, or even "benign" (e.g., a hardware malfunction). And they may occur at any time. Also, once they occur, the damage they cause may spread and multiply with incredible speed. Accordingly, to minimize the likelihood of any breach and to mitigate its consequences, LSPs need to be vigilant. Careful real-time monitoring of employee practices can help ensure compliance with the LSP's privacy and security policies and better safeguard information both within an organization and in the hands of any contractor or other third party.

Comment 6b: Organizations differ, often substantially, in size, scope, the nature of the data retained or transferred, and attendant threats, both internal and external. Accordingly, each LSP should establish a mechanism for assessing the various components of its information security environment, program,

and policies, including those relating to physical security, information access controls, intrusion prevention and detection systems, encryption technologies, and the maintenance, transfer, and disposition of information. For some providers, such monitoring may be relatively simple and straightforward. Others may need to employ, depending on their industry or situation specific requirements, standard auditing frameworks, such as SSAE 16 (formerly SAS), the ISO 27000 series standards, or a framework capable of being measured, assessed, and improved with demonstrable and documented criteria and according to a fixed schedule. Of course, as technology changes, so will these lists.

Comment 6c: Ultimately, an organization is responsible for the confidentiality, integrity, and availability of information under its possession, custody, or control. Implementing a reasonable auditing regime that evaluates policies and procedures governing its information assets and properties demonstrates a reasonable and prudent management philosophy to address a complex and evolving field.

Principle 7: Legal service providers should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

Comment 7a: Threats to security and privacy change constantly. The compliance landscape, arising from industry-specific, state, and federal requirements, or obligations that affect the creation, management, transfer, or disposition of information in non-U.S. jurisdictions, challenges organizations at every level. These factors, coupled with constantly evolving technologies, require ongoing vigilance to ensure that the LSP's privacy and security policies and practices remain responsive to changing circumstances.

Comment 7b: To be "reasonable and appropriate," security policies and practices should be current; and the best way to keep them current is to stay abreast of developments, reassess risks, and update the policies and practices as needed. This suggests a need to perform two tasks in tandem: (1) conduct *ad hoc* assessments based on active monitoring of the LSP's actual real-time or near real-time practices; and (2) undertake regularly scheduled (ideally annually) reviews of technological developments that may concern the LSP's current internal practices or supported programs. *Ad hoc* assessments are proactive measures undertaken by, or under the direction of, the person who is responsible for implementing and enforcing the LSP's security policies and practices.

Comment 7c: The person responsible for *ad hoc* assessments must be qualified to do the job directly, or have the authority and budget to engage expert consultants to perform the assessment. Additionally, that person should have the authority to effect change directly to reasonably address any identified defects in the policies or practices. To minimize the possibility of missing important developments, LSPs need to follow-up its assessments with regularly scheduled reviews of the entire security program and, where necessary, update the policies and practices as risks and best practices evolve.

II. SOURCES OF THE DUTY TO PROTECT PRIVATE AND CONFIDENTIAL INFORMATION[3]

The duty to protect privacy applies to all participants in the legal services industry. The principal sources of the duty are found in: (1) ethical rules applicable to attorneys; (2) federal and state statutes and regulations; (3) foreign laws, where applicable; (4) common law; and (5) client choices, including contractual obligations imposed by the client.[4]

A. Ethical Rules Applicable to Attorneys

1. Model Rules 1.1, 1.6, and 1.18

ABA Model Rules of Professional Conduct 1.1 and 1.6 require attorneys using technology to take competent and reasonable measures to safeguard client information. This duty extends to the use of all technology, including computers, mobile devices, networks, technology outsourcing, and cloud computing.

Rule 1.1 requires "[a] lawyer [to] provide competent representation to a client." This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." It includes competence in selecting and using technology. In August 2012, the ABA House of Delegates added a

3. Unless otherwise expressly stated in this Commentary, the term "information" includes both electronically stored information ("ESI"), as well as information in paper or hard-copy form.

4. This Commentary is not intended to establish a "duty of care" imposed upon LSPs. Rather, it is designed to identify issues relating to the protection of client and third-party private and confidential data and, most important, articulate practices that should be considered in protecting such data. To that end the technology and threats in this area are constantly changing. LSPs should adapt their practices to safeguard private and confidential information of their clients and third parties taking into account the evolving technologies and threats.

comment to Rule 1.1 that imposes an additional professional competency responsibility to keep "abreast of changes in the benefits and risks associated with relevant technology" as the changes relate to the law and to legal practice.

Attorneys' use of technology presents special ethical challenges in these areas of competence and confidentiality. The duty of competence requires attorneys to know what technology they need and how to use it. If an attorney lacks the necessary technical competence for security, he or she must consult with someone who has the requisite expertise.

ABA Model Rule 1.6 regarding client confidential information is one of the most challenging ethical responsibilities when it comes to technology. All fifty states and the District of Columbia have an ethical rule prohibiting (subject to certain exceptions) a lawyer from revealing information related to the representation of a client unless the client provides informed consent. The ABA's Comments to Rule 1.6 specifically address a lawyer's obligation to preserve confidentiality, requiring lawyers to act competently to safeguard information relating to the representation of a client. Lawyers have the same duty to safeguard the confidential information of prospective clients, per Rule 1.18.

Twenty-nine states and the District of Columbia have issued comments to Rule 1.6 requiring that attorneys take "reasonable precautions" to prevent unauthorized access to client communications. The comments provide that attorneys generally do not need to take "special security measures if the communication affords a reasonable expectation of privacy," but note that special circumstances may warrant special precautions. Relevant factors include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or a confidentiality agreement. However, many states have issued separate ethics opinions based either upon

Rule 1.1 or state versions of that Rule, in addition to other Model Rules discussed below. These ethics opinions often introduce additional requirements—such as suggesting the type of contractual terms required between a lawyer and cloud service provider, or the types of background investigations that lawyers should require of their cloud providers—as preconditions for ethically arranging to store client information in the cloud. The ABA maintains an online chart listing these opinions.[5]

2. Model Rules 4.4 (a) – (b)

Lawyers also have a duty to protect the confidential information of third parties, including adversaries. Model Rule 4.4 (a) provides that, in representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or knowingly use methods of obtaining evidence that violate the legal rights of such a person, including privacy rights. Rule 4.4 (b) relatedly requires a lawyer to notify the sender if he or she receives a document or electronically stored information relating to the representation of the sending lawyer's client and if he or she knows or reasonably should know that the document was inadvertently sent.

3. Model Rules 5.1, 5.3, and 5.7

Lawyers are responsible for the professionals they hire and should have reasonable checks in place to ensure confidentiality and good hiring practices. Model Rules 5.1 and 5.3 incorporate into the lawyer's professional obligations the duty to supervise the work of subordinate attorneys and non-attorneys, agents, and TPSPs, including those outside the firm. Those rules

5. *See Status of State Review of Professional Conduct Rules*, AMERICAN BAR ASSOCIATION (Sept. 14, 2011), http://www.americanbar.org/content/dam/aba/migrated/cpr/pic/ethics_2000_status_chart.authcheckdam.pdf.

require lawyers with managerial responsibilities to make reasonable efforts to ensure that those working for them act in a manner compatible with the professional obligations of the lawyer. Model Rule 5.7 further extends the lawyer's professional responsibilities to apply to law-related services.

Comment 3 to Model Rule 5.3 expressly refers to a lawyer's use of outside technology services[6] and cautions that the degree of due diligence required to vet and supervise these contractors "will depend upon the circumstances, including the education, experience, and reputation of the non-lawyer, the nature of the services involved, the terms of any arrangements concerning the protection of client information, and the legal and ethical environments of the jurisdictions in which the services are performed, particularly with regard to confidentiality."[7] The state ethics opinions that address the use of cloud services to store client information are not entirely consistent with each other.[8] Lawyers with multi-state practices will be subject to the ethical standards of every state in which they practice. For those lawyers using cloud services for storage of client information, no ethics opinion has yet addressed whether the laws and legal ethics standards of the jurisdiction in which the cloud

6. *See* ABA MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. (2013), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/comment_on_rule_5_3.html.

7. *See* ABA Comm'n on Ethics 20/20, *Report to the House of Delegates Resolution 105C*, AMERICAN BAR ASSOCIATION, http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.authcheckdam.pdf (last visited June 2, 2015).

8. *See Cloud Ethics Opinions Around the U.S.*, ABA LEGAL TECHNOLOGY RESOURCE CENTER, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited June 2, 2015). A detailed comparison of these different state ethics opinions is beyond the scope of this paper.

provider's servers are located, also apply to the "foreign" lawyer who arranges for the cloud storage service.[9] Finally, U.S. government attorneys are "subject to State laws and rules, and local Federal court rules, governing attorneys in each State where such attorney engages in that attorney's duties, to the same extent and in the same manner as other attorneys in that State."[10]

B. Federal Statutory Obligations

The U.S. has taken a sectoral approach to privacy issues, which adjusts protections to particular circumstances and regulatory regimens.[11] A comprehensive discussion of all sectoral requirements is beyond the scope of this Commentary. However,

---

9. The laws of non-U.S. jurisdictions where cloud servers are located might also govern the precautions required for protecting client data. A practitioner should carefully consider and discuss with the client the advantages and disadvantages of storing data outside of the client's home state, as well as outside of the U.S. Even aside from the likelihood of different legal and ethical standards applying outside of the U.S., in some non-U.S. jurisdictions where servers might be located, there could be no effective legal protections at all, subjecting client data to the risk of sale to the highest bidder by the cloud service provider, by corrupt employees, or by officials.

10. McDade Act, 28 U.S.C. § 530B(a) (2012), https://www.law.cornell.edu/uscode/text/28/530B (last visited June 2, 2015) ("Ethical standards for attorneys for the Government").

11. A reference to a few of the federal statutes implicating privacy suggests the range and variety of ways in which the federal government addresses the issue:

- Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510
- Driver's Privacy Protection Act (DPPA), 18 U.S.C. §§ 2721–25
- Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681
- Fair Debt Collections Practices Act (FDCPA), 15 U.S.C. §§ 1692–92
- Financial Services Modernization Act (GLBA), 15 U.S. Code §§ 6801–10

the laws and regulations that govern two particular industries, health care and financial services, are worthy of mention because they serve as useful models. Both industries operate within a regulated framework that: (1) imposes security standards on industry members; (2) requires special service contracts between those who collect information from consumers and those who provide services to them; (3) requires notification to consumers when security lapses result in the loss of information pertaining to a non *de minimis* number of consumers; and (4) subjects those who lose data to potential legal liability. It is also worth examining the laws and regulations applicable to these two industries because most LSPs will handle financial or health related information in the course of providing legal services, so it is important to understand the restrictions applicable to such information. Therefore, a brief discussion of the privacy regulations that govern those two industries is included in Appendices A and B.

C. State Regulations

The unauthorized disclosure of personal information may trigger state data breach laws that require notifying consumers, governmental agencies, or both. A data breach may also result in regulatory investigations and penalties. Indeed, many

---

- Health Insurance Portability and Accountability Act (HIPAA), 42 U.S. Code § 300gg
- Stored Communications Act (SCA), 18 U.S.C. § 2701
- Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710

Although it is not exhaustive, this list illustrates the U.S. patchwork of federal privacy laws that imposes different sets of duties. In addition, there are literally "[t]ens of thousands of record retention legal requirements" that are imposed by "the federal government, the fifty states, the District of Columbia, and the U.S. territories." Many of these implicate privacy issues. Peter Sloan, *The Compliance Case for Information Governance*, 20 RICH. J.L. & TECH. 4, ¶ 8 (2014), *available at* http://jolt.richmond.edu/v20i2/article4.pdf.

data breach laws require that notice be provided to the state Attorney General.

Nearly all states, the District of Columbia, Puerto Rico, and the Virgin Islands require notice to their residents in the event a resident's personally identifiable information (PII) is breached. Most of these laws have a "risk of harm" trigger, requiring notice only if it is determined, after a reasonable investigation, that there is a reasonable likelihood of harm to consumers. However, some states, including California and Massachusetts, do not limit the notice requirement in this way.

Apart from the broad definition of PII used in this Commentary (*see supra* note 1), the definition of PII varies among the states and territories, but generally includes a resident's first or last name, combined with one nonpublic identifier, such as a social security number, state ID, driver's license number, credit card number, or bank account number. The majority of these laws are limited to electronic information, but at least six states (Alaska, Hawaii, Indiana, Massachusetts, North Carolina, and Wisconsin) apply the laws to paper records as well.[12]

Some state laws also impose minimum security requirements, including requirements for a written information security program (commonly known as a WISP), and for encryption of personal information that will travel across public networks, be transmitted wirelessly, or be stored on laptops or other portable devices.

LSPs should develop an incident response plan that addresses their potential duties, and be knowledgeable about applicable laws, considering, for example, that these laws may

12. This is a very active area of state-level legislation. Many states are actively enacting and revising these laws, and LSPs therefore need to stay on top of developments. *See, e.g.*, Florida Information Protection Act of 2014 (FIPA) (2014), http://laws.flrules.org/2014/189.

apply to a client's information that is stored on the LSP's network or a cloud provider's network, even if the client and lawyer do not have any other contacts with the state.

D. Foreign Statutory and Regulatory Requirements

International privacy is a dynamic area of the law in which consumers, private entities, and government actors seek to balance the considerable benefits of technological innovations with critical privacy concerns. Disclosures of national security inquiries—the "Snowden effect"—and other large-scale data breaches have forced privacy issues into the forefront and instigated unprecedented activity in the development of data protection regulation. These developments will profoundly affect the way global businesses and their LSPs approach the collection and management of personal information.

The state of the law in the European Union (EU) is in flux even as this Commentary is being completed; and the impending adoption of a new EU data protection regulation will fundamentally change the existing EU framework. On March 12th, 2014, the European Parliament voted to continue revising and strengthening the draft regulation. Among other things, the proposal: (1) implements new protections concerning the transfer of EU citizens' information to non-EU countries; (2) significantly increases the potential fines to corporations in breach of the regulation; (3) guarantees the right to be forgotten; (4) incorporates the theme of information "portability" to support greater control by individuals; (5) unifies inconsistent and diverse nation-specific laws into one "pan European" data protection law; and (6) mandates incorporation of privacy by design into products and services. The General Data Protection Regulation will next be considered by the Council of Europe, which consists of representatives of twenty-eight EU governments.

They are tasked with considering and ultimately, in negotiations with the EU Parliament, agreeing to a single set of proposals.

Equally significant, stronger cross-border privacy rules are also being developed in Latin America and Asia. Countries as diverse as Costa Rica, Brazil, South Korea, Hong Kong, and Singapore have recently adopted, or are considering adopting, broad-based data privacy laws. Canada is also considering significant new privacy legislation.

E. Common Law Liability

A discussion of all potential theories of common law liability for data breaches is beyond the scope of this Commentary. Nonetheless, a few are worth highlighting; these include: (1) legal malpractice; (2) breach of fiduciary duty; (3) breach of contract; and (4) general tort, including class action negligence claims.[13] For example, an LSP who loses a client's confidential information may not only be accused of breaching his or her ethical obligations, but may also be subject to claims of legal malpractice and breach of contractual duty (express or implied) to safeguard client information. Similarly, third parties whose identities are stolen or who are otherwise injured by a loss of sensitive personal information may seek legal redress for their injuries. One need only consider the class actions that have followed major data breaches to appreciate the business case for taking adequate steps to secure sensitive information, no matter whose information it is.

---

13. One study "identified over 86 unique causes of action" from a universe of 231 cases. *See* Sasha Romanosky et. al., *Empirical Analysis of Data Breach Litigation* (Apr. 6, 2013) at 25, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461 (Forthcoming in the Journal of Empirical Legal Studies; Temple University Legal Studies Research Paper No. 2012-30).

F. Client Choices

A broad range of information security decisions may be left to the client's business judgment. The client always has the discretion to make business decisions about which providers to engage based upon risk assessment of the providers' information security. Although the client ultimately pays for the security measures, it is not the only one who is potentially liable for any loss of third-party information.

When counseling clients about security alternatives, the LSP should document any advice and ensure that the client has access to technology experts. Upon request from the client, the LSP should clearly disclose the nature of the security measures and policies of the firm. Any decision by the client to forego security measures that the LSP recommends should be documented. In addition, the LSP should, when appropriate, counsel the client about potential liability insurance coverage issues and be mindful that in some situations (especially those that may expose the LSP to third-party lawsuits) the LSP should consider whether to decline to provide representation.

III. CONDUCTING A SECURITY RISK ASSESSMENT

The touchstone of a sound information privacy and security program is its careful tailoring and scaling to the LSP and its practice. This tailored approach begins with an assessment of risk, considering both the probability and the harm or damage that could be caused by an occurrence.[14] LSPs should determine what privacy and security solutions are appropriate to the circumstances using a risk-based analysis,[15] and subsequently develop and implement a reasonable and appropriate information privacy and security program to mitigate risks.

The Homeland Security Act refers to "information security" as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: A. Confidentiality, B. Integrity, and C. Availability."[16] Thus, to properly assess the risk, an LSP must consider the importance of maintaining the confidentiality, integrity, and availability ("CIA") of the information it possesses.[17] By these terms we mean:

- Confidentiality: protecting the information from disclosure to unauthorized parties;

---

14. *See* National Institute of Standards in Technology, Special Publication 800-30, *Guide for Conducting Risk Assessments*, NIST (Sept. 2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [hereinafter *Guide for Conducting Risk Assessments*].

15. Valerie Fontaine, *The New Lawyer - What size fits me?*, DAILY JOURNAL, Nov. 26, 2013, https://www.dailyjournal.com/public/Pubmain.cfm?seloption=The%20New%20Lawyer&pubdate=2013-11-26&shNewsType=Supplement&NewsId=965&sdivId=&screenHt=680&eid=932352.

16. 44 U.S.C. § 3542(b)(1) (2012), https://www.law.cornell.edu/uscode/text/44/3542 (last visited June 2, 2015).

17. For a more detailed look at how each of these components can be considered and evaluated, *see infra* Table 1 in Section III.C.

- Integrity: protecting information from being modified by unauthorized parties; and
- Availability: ensuring that authorized parties are able to access the information when necessary.

Absent an intentional alteration, information an LSP has on hand should, at all times, be the same information that it either generated or received. If it is private or confidential information, it should be protected from those who do not need to see or use it. Those who must use it, must be able to obtain it quickly whenever they need it.

In security terminology, the basic elements common to almost every risk assessment are:

- Asset Identification and Evaluation: Identify assets and evaluate their properties.
- Risk Profiling and Assessment: Analyze the specific threats and vulnerabilities that pose the greatest risk to information assets.
- Risk Mitigation and Treatment: Develop reasonable responses to the threats and vulnerabilities identified. The practices discussed in Section IV of this Commentary provide a guide for such risk mitigation efforts.

A. Asset Identification and Evaluation

During this first stage, the LSP should identify the types of information it handles generally or will handle in conjunction with a specific representation (e.g., social security numbers, payment card numbers, patient records, designs, and human resources data), evaluate the sensitivity or relative importance of each type of information, and rank by priority which types require protection.

In identifying information assets and developing priorities, LSPs should do the following:

- Consider the sources and nature of the information, along with where it resides or will reside. This may include data created by the LSP and client-created data stored by the LSP—both of which may have different security concerns and security requirements.
- Identify and list where each item on the information asset list resides or will reside within the organization (e.g., file servers, workstations, laptops, removable media, PDAs, phones, databases). If information will be stored outside the organization (such as with a cloud service provider), the LSP should note that as well.
- Categorize information and rank each category based on its degree of sensitivity and risk. For example, an LSP might decide to categorize its information and rank it as follows:
    1. Public information, either belonging to the LSP itself or a client (e.g., marketing campaigns, contact information, public financial reports, etc.)
    2. Internal, but not secret, information belonging to the LSP (e.g., phone lists, organizational charts, office policies, etc.)
    3. Sensitive internal information belonging to the LSP (e.g., business plans, client lists, strategic initiatives, items subject to non-disclosure agreements, etc.)
    4. Confidential client information subject to the attorney-client privilege or work-product protection

5. Regulated information belonging to the LSP or its client (e.g., patient data, classified information, etc.)
6. Compartmentalized internal information belonging to the client or the LSP (e.g., compensation information, certain highly sensitive client information that is not to be generally accessible to all of the LSP's personnel, HR data, etc.)
7. Private or confidential information of a third party (e.g., the LSP may have received private or confidential information pursuant to court discovery)

- Evaluate client requirements. Many clients have their own security requirements and will want their LSPs and TPSPs to comply with them. A growing trend among clients is to require LSPs to self-certify that they meet security requirements and submit to security audits by an independent party.
- Regardless of whether clients have formal requirements for information privacy and security, LSPs should discuss with them the nature of the information expected to be involved in any representation. LSPs should then plan to provide the appropriate level of security.
- Fundamentally, and regardless of the category or ranking chosen, the LSP should rank information assets based on:
    1. the sensitivity of the information;
    2. the threats posed by third parties or internal lapses;

3. the vulnerability of the information to the identified threat; and
4. the amount of harm that would be caused if the information were disclosed or altered. For example, client information with great economic or political value is more likely to be targeted by thieves than information having little or no value to anyone except an individual client.

- Evaluate third-party requirements. Many LSPs receive information belonging to a third party, such as an opponent or witness. The LSP has the same obligations to protect the privacy and confidentiality of that information when it was obtained through the discovery process. This may require the LSP to discuss with its opponent and enter into appropriate written agreements or orders regarding the handling of that information during the litigation and the disposition of that information at the end of the litigation.

B. Risk Profiling and Assessment

During this stage of the risk assessment process, the LSP should rate not only the sources of risks and specific threats (for example, those identified above) facing its most valuable or sensitive information assets, but also the organization and its IT infrastructure more generally.

Sources of risk can include the following:

- The LSP's Physical Infrastructure

  The potential for security problems varies greatly among LSPs. The number of LSP employees and contractors, their relative (in)sensitivity to security issues, the number of offices the

LSP maintains, and the amount and nature of the information the LSP holds all tend to affect the risk of security breaches and influence the level of any necessary privacy and security programs. Understanding confidentiality, integrity, and availability in this context requires an analysis of existing policies and security measures that address information disclosure, unauthorized information release, and appropriate access to data. Using this analysis, LSPs should confirm the reasonableness of existing information security practices and whether they need to implement different or additional measures.

- Existing Firm IT Systems

  An LSP should assess the potential points of weakness or penetration in its existing IT infrastructure as well as that of any third party involved in providing IT services or infrastructure. This assessment should not only look at the formal IT infrastructure of the LSP, but also other systems that may interface with that infrastructure such as smart vending machines; heating, ventilating, and air conditioning systems; or other devices that are in any way connected to the LSP's network and thus offer a potential point of penetration. Weaknesses can also be the result of TPSPs who have access to the LSP's network or who provide contractors to assist the LSP's IT department. Here, a CIA assessment for IT systems may aid the evaluation of the security of the physical and technical infrastructure of the LSP, including its ability to

protect data from intruders and to provide appropriate data access internally. Finally, this analysis should consider LSP disaster recovery locations.

- The Practice Needs of Attorneys (e.g., travel, work from home, remote access)

  Modern legal practice and the level of responsiveness expected by clients require LSPs to access information through extranets, mobile devices, or other devices while working from home or traveling outside the office. However, remote access can increase risk. When performing a risk assessment here, providers should consider whether employees are able to access the information they need while ensuring that data is not modified and is inaccessible to unauthorized people. LSPs should address the potential for data loss via use of BYOD devices, flash drives, cloud applications, or sending data to personal e-mail.

- Vendors or Cloud Storage Providers

  Many LSPs rely on third-party vendors to host data. Similarly, LSPs are moving towards cloud-based service providers or applications that will inevitably store firm, client, and third-party data. The LSP has the same responsibility to ensure the protection of data to the extent that it has engaged the particular vendor or service provider. This may include evaluating the service provider's security and ensuring that any necessary protection is implemented by the vendor or service provider.

When using third-party or cloud services, LSPs should consider storing data in an encrypted form. Two types of cloud encryption services are available, standard shared-key and personal or zero knowledge. With standard encryption, the third-party vendor will know the client's encryption key. Zero-knowledge encryption is considered to be more secure because the vendor will not have the encryption key. The idea is that anyone accessing the data through the vendor will not be able to decrypt it.

- Possession of Valuable Information (client or LSP's)

  The more valuable the information an LSP possesses, the greater the incentive someone has to try to steal it. In this context, providers should analyze and evaluate their inventory of information at frequent intervals to ensure that reasonable security needs are in place.

  When creating a risk profile, LSPs should always keep the CIA assessment in mind.[18] This analysis should include known vulnerabilities; for example: the potential for inadvertent data breach due to employee error or negligence, external hacking, denial of service/loss of access, employee theft, loss of data due to equipment failure, disruption of communications and power, or even natural disasters. For each risk/threat identified, the next step is to assess the probability of the threat actually occurring

18. *See Guide for Conducting Risk Assessments*, *supra* note 14.

and the consequences if the information is lost, stolen, or improperly disclosed.

C. Risk Mitigation and Treatment

Once the sensitivity of information assets has been determined and the sources of risks and threats identified and ranked, an LSP is in a position to make informed decisions regarding how best to protect information. For example, an LSP may decide to store certain client documents in its own document management system for convenient access by a large case team, where such documents contain stale business information that would not have a substantial negative impact if lost. In contrast, the LSP might erect significant access barricades around highly sensitive client trade secrets or the client's customers' private information, where the loss of the information would have severe, or even catastrophic, consequences. There will always be a need to balance convenience and function with security. Too much security can impede the ability of attorneys and TPSPs to do their jobs, while too-little security risks exposing sensitive information belonging to the LSP, its clients, or third parties. For a more detailed look at how varying security objectives might be weighed against varying levels of risk, see Table 1, *infra*.[19]

All LSPs should consider scaling and prioritizing their information security practices to fit their particular circumstances as they are known at the time. The focus should always be on what is reasonable and appropriate. To determine that, an LSP should first evaluate the type of information it has, who uses the information, and how they use it. The LSP should also consider CIA: which of its employees should have access to information,

19. *See also* FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, NIST (Feb. 2004), http://infohost.nmt.edu/~sfs/Regs/FIPS-PUB-199-final.pdf (last visited June 2, 2015).

when they should have it, and whether they have put in place effective measures to prevent unauthorized access. All providers have challenges ensuring security for private and confidential information, but ultimately all need to scale their security programs to meet their own and their clients' needs.

POTENTIAL IMPACT [Table 1]			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C. § 3542(b)(1)]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C. § 3542(b)(1)]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C. § 3542(b)(1)]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

IV. GUIDELINES FOR POLICIES AND PRACTICES THAT ADDRESS PRIVACY AND INFORMATION SECURITY

Information security practices should be scaled to the circumstances of the LSP and the needs of its clients. They may be simple or complex. This section of the Commentary sets out a multi-faceted and layered approach to information security.

Not everything set out in this Section can or should be adopted by everyone. Rather, the Section identifies a variety of policies, practices, and methods that might be used to meet the needs of LSPs and clients. Providers should consider cost, business needs, and strategy, but ultimately the reasonableness of the solution is derived from the results of the LSP's risk assessment described in Section III.

This Section IV describes certain processes and practices by which members of the legal services industry may:[20]

---

20. Of course, there is more than one way to set up a program. For example, the FTC's Standards for Safeguarding Consumer Information direct those subject to the Gramm-Leach-Bliley Act, 15 USC §§ 6801(b), 6805(b)(2), to do the following:

> (a) Designate an employee . . . to coordinate . . . information security;
>
> (b) Identify reasonably foreseeable internal and external risks . . .
>
> (c) Design and implement . . . safeguards to control the risks . . .
>
> (d) Oversee service providers . . .
>
> (e) Evaluate and adjust . . . [the] information security program in light of the results of testing and monitoring [the program]. . . .

16 C.F.R. 3.14.4. The CFTC has issued similar guidance to those subject to its jurisdiction. *See* Gary Barnett, *CFTC Staff Advisory No. 14-21*, U.S. COMMODITY FUTURES TRADING COMMISSION (Feb. 26, 2014), http://www.cftc.gov/ucm/groups/public/@lrlettergeneral/documents/letter/14-21.pdf.

- consider the sources of the sensitive information they maintain and the nature of that information;
- identify those within the organization with a bona-fide need for access to information and limit access to those people;
- address information security policies in three subparts:
    1. information security in the office and on the network
    2. information security for information that travels outside the office or the network
    3. information security for information that is shared with experts, consultants, other service providers, and adversaries (either in negotiations or discovery exchanges);
- plan for the disposition of information after it is no longer needed;
- institute a training program that reaches everyone and incentivizes their compliance; and
- anticipate potential breaches by developing plans for prevention, improving detection and response to incidents, preparing to notify affected parties if the information is jeopardized, and adopting contingencies for promptly resolving any problems.

A. Step 1: Identify the Types and Sources of Information That Must Be Protected

To launch any privacy and information security program, an LSP should first evaluate the type of information it has and collects as well as how it uses that information. LSPs are

repositories of lawyer-created information and client information, as well as information concerning third parties. Information that may be used for litigation may need to be treated differently than information that may be used to facilitate basic legal advice or business transactions. Security precautions for client information may already be addressed in retainer agreements—a salutary practice—particularly, if client information is to be stored off-site, including in the cloud. Security for third-party information may often be governed by contract or court order.

B. Step 2: Determine Those Who Need Access

The LSP should determine who among its members and employees needs to have access to what information and under what circumstances should they have it—keeping in mind that all security breaches and leaks come from one of three possible sources: (1) employees (whether intentionally or inadvertently);[21] (2) lost or stolen media; and (3) intrusions from the outside. The governing information management principle should be "need to know." Only those employees with a specific business purpose requiring access to a particular type of information should have access.

---

21. One article identifies four types of employees who pose risks: the "security softie" who does things he or she should not do; the "gadget geek" who adds devices or software to the system that do not belong there; the "squatter," who uses IT resources inappropriately; and the "saboteur," who hacks into areas where he or she does not belong. The article further notes that "insider threats come from many sources: maliciousness, disgruntled employees, rogue technology, lost devices, untrained staff and simple carelessness." *See* Mark Hansen, *4 types of employees who put your cybersecurity at risk, and 10 things you can do to stop them*, A.B.A. J., Mar. 28, 2014, *available at* http://www.abajournal.com/news/article/war_stories_of_insider_threats_posed_by_unapproved_data_services_and_device.

C. Step 3: Information Security Policies and Practices

This section addresses information security policies and practices in three distinctly different contexts: security in the office and on the network; security for information outside the office or network; and security for information when it is provided to others. In each of these three situations, a fully adequate information security and privacy program can be scaled to meet the specific needs of the LSP and its clients.

1. Security in the Office and on the Network

a. Physical Security of the Office

Policies should provide for physical security of the LSP's office, including when doors should be locked, who has access to main entrances, offices, conference rooms, storage rooms, and other office locations. For example, a policy might specify that office locations, whether desk drawers, file cabinets, or file rooms, that contain confidential information be locked when not in use, and access should be limited to people who need access. A slightly more elaborate plan may require that all access to areas containing confidential information should be tracked, perhaps through sign-in sheets or, more elaborately, through electronic verification such as keycards. An even greater level of security might require that servers or records storage areas should have especially limited employee access, perhaps deploying security cameras inside and outside these areas, or an intrusion alert system. Biometric checkpoints may be warranted in some special circumstances.

b. Network Security

Once an LSP has a single computer connected to a server, WiFi router, or other network-enabled device, it has a network. At a minimum, that network should then be protected against failure, and if it is connected at all to the outside world, it should

be protected against intrusion. Network security requires developing secure infrastructure either in accordance with a client's specific security needs or according to a standard industry benchmark.[22] While the level of security is certainly scalable to fit the circumstances, once a provider moves beyond the most basic level, it will likely need to determine who will monitor the firm network for security breaches, how that monitoring will be accomplished, and how the monitors will be monitored. Policies should describe procedures for regularly monitoring and analyzing network logs and events, and for identifying and addressing potential security breaches. Audits and monitoring are more specifically discussed in Part IV.C.1.h., *infra*.

---

22. Industry certifications can represent a useful benchmark, but LSPs should generally not consider certification, or lack of it, to define the level of security. In addition, providers relying on these or other industry standards to determine third-party security should inquire as to exactly which parts of the third party's business are certified and which are not certified.

ISO is the largest developer of standards in the world. Its membership is drawn from the National Standards Bodies of multiple countries. The International Electrotechnical Commission oversees the development of electrical and electronic Standards for participating countries. The 27000 series has been reserved specifically for information security matters. ISO 27001 is a standard describing the best practice for an Information Security Management System, often referred to as "ISMS." An ISMS is "part of the overall management system, based on a business risk approach, to establish, implement, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, processes and resources." ISO/IEC 27000: 2012.

SSAE-16 (Statement on Standards for Attestation Engagements No. 16) is also a commonly used security standard for data centers, as set forth by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA).

c. Secure Backup

Information security policies should provide for secure backup of provider information and include disaster/recovery plans, including procedures for restoration. LSPs should consider off-site storage of encrypted backup media, and if they backup client information separately from their own information, these backup processes should also have disaster/recovery plans. Such plans would ideally include specific procedures for backup and restoration that are understood, agreed upon, and maintained in compliance with a written agreement among the clients, providers, and third parties (as appropriate). Conducting regular test restores is highly recommended.

d. User Authentication and Permissions

LSPs can only protect private and confidential information that is stored on networks or on devices by requiring those who seek access to the information to show they have authorization to access it. This means that access to information stored on a network, a computer, or a mobile device should require user authentication through such means as passwords or, in the case of multifactor authentication, a password combined with a security question. Similarly, assuming the provider determined, in Step 2, that employee and partner access to certain information should be restricted, then users' access should be limited through permissions for designated levels of sensitive information. For example, an LSP might implement role-based access controls (RBAC) by which its employees' access to information would be determined by the type of information and the employee's role in the organization. Such a system might grant varying rights depending on whether a person is a partner, associate, litigator, secretary, and so forth.[23]

23. For an overview of the subject, *see Attribute Based Access Control (ABAC) – Overview*, NIST, http://csrc.nist.gov/projects/abac (last visited June

No matter how the LSP grants or limits access to particular types of information, access to network areas and devices containing confidential information should be protected at least by "strong" passwords. "The strength of a password is related to its length and its randomness properties."[24] Strong passwords should be of sufficient length and complexity so that they cannot be guessed, e.g., they should contain a combination of capital and lowercase letters, numbers, and special characters. Users should change login passwords regularly. Although at times inconvenient for the user, ideally a network would also lock out a user who has not revised a password within a prescribed interval, or who has failed to enter a correct password after several incorrect attempts.

e. External Media

While there might be valid reasons to use external media such as flash drives, transferring information to portable media can compromise security. The media could introduce viruses or malware to the network. Information copied onto peripheral media can create an additional risk point because the media can easily be transported, lost, or stolen.

2, 2015). For a more detailed review of the topic, *see* David F. Ferraiolo & D. Richard Kuhn, *Role-Based Access Controls,* 15th National computer Security Conference (1992), Baltimore MD, pp. 554–563, *available at* http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf. An alternative, more complicated, system for limited access controls is the attribute based access control (ABAC). For an overview of this method, see *Attribute Based Access Control (ABAC) – Overview*.

24. *See* Meltem Sönmez Turan et. al., *Special Publication 800–132*, *Recommendation for Password-Based Key Derivation*, *Part 1: Storage Applications*, NIST, Appendix A.1 (Dec. 2010), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf [hereinafter *Recommendations for Password-Based Key Derivation*].

Thus, policies should restrict the use of unencrypted external media. LSPs should consider policies that specify when any external media may be used, who may use it, to what devices it may be connected, and how it is to be stored, erased, reused, transferred, and designated for disposal. Such "policies" can take several forms, from written directives to technical measures that preclude transferring or copying information. LSPs should encrypt portable media to restrict unintended access.

f. Remote Access of Provider Network

Many LSPs permit employees to access their network from locations outside the office. This access may be through encrypted connections such as Virtual Private Networks (VPN) or remote access programs in order to maintain privacy and security. Remote access with authentication via two levels of passwords and deployment of access controls through RBAC or attribute based access control (ABAC) should ensure that those with permission to access certain information are the only people who can access it.[25]

LSPs that offer WiFi access in their office should ensure that the network is protected through over-the-air authentication and encryption, and their policies should provide protocols for managing and monitoring the WiFi network. Logging features should be enabled so that there is a record of everything that is copied, in the event that data is wrongfully accessed. Wireless networks should be encrypted and LSPs should not overlook the security of their wireless network (current WiFi Protected Access II (WPA2) provides the highest level of router protection). Guest WiFi should be provided through a separate network with no ability to access the rest of the network.

---

25. *See Recommendations for Password-Based Key Derivation*, *supra* note 24 and accompanying text.

LSPs should train employees to avoid publically available computer systems, such as computers at hotels, when accessing the LSP's network. Unless the system is merely a dumb terminal without capacity to save or further transmit information, any restrictions on further use and dissemination become problematic, and accountability for the information is compromised. Even if the employee is personally trustworthy and loyal, the LSP should consider whether the employee should be allowed to use the devices of friends and family members to access the provider network or use public networks such as cafes or airports. Private or confidential information may be stored on the device and accessed by an unauthorized person.

g. Receipt and Creation of Confidential Information

Although very difficult to achieve in practice, LSPs should consider implementing detailed procedures to track client information from receipt until destruction. Such procedures might establish a central point for receiving and tracking client or case-related information and implement a process for logging information received from the client, no matter whether it arrives on an electronic device or external media, through an online transmission (email, ftp site, web file sharing service, etc.), or in hard copy. Logging the date, sender, recipient, and contents of information received facilitates managing the information. Attaching a label with a unique ID to each piece of any media, device, or hard copy file received may also help manage them throughout the representation. Logging confidential information allows LSPs to begin a chain of custody that reflects access, copying, transfer, and deletion of the files.

LSPs should also consider whether there is a need to distinguish between client-created information that is sent to them and work product that is generated by the LSP. Although LSPs should treat both types of information as confidential, the LSP

may find it easier to create distinct lifecycles for provider-created information and client-created information for the purpose of chain of custody and work management, as well as disposition at the end of a matter.

h. Monitoring and Audits

Oversight is appropriate to ensure that policies are executed correctly to identify remaining areas of risk and to quickly identify breaches. Policies should address who is responsible for audits and how and when audits will be conducted and reported. Monitoring should include all areas of the LSP's business and all processes involving confidential information, although they need not all take place at the same time. Checklists can serve as a useful guide to ensure thoroughness of past and future audits.

In addition, real-time tracking and accounting of client information is necessary to identify breaches quickly and help mitigate problems caused by data loss. Immediate notification of appropriate LSP partners and affected clients, as well as any third parties, such as law enforcement authorities or insurers involved in the transport or loss of information, is essential.

LSPs should also include a requirement for periodic data inventories, e.g., determining what information the LSP has and where it resides. Regular checks on data logs and data inventories provide quality assurance of information security.

2. Security Outside the Office and Network

Whenever information moves, it is vulnerable to being damaged, lost, stolen, or altered. This is true whether a move entails a ride in a cab to the courthouse or a trip around the globe for a meeting. Information security programs should consider the movement of information and the potential risks. Where information is subject to special requirements, the LSP should set

forth a mechanism for alerting the relevant personnel to those requirements.

a. Encryption of Copies and During Transfers

LSP policies should generally require encryption when private or confidential information is transferred. Unless email is encrypted, LSPs may wish to consider alternative ways to transfer particularly sensitive, private, or confidential information. Encryption is more than a useful and convenient information security tool. It is critical for protecting client information, especially when the information is stored on mobile devices, transmitted, or stored remotely. Typically, encryption applies an algorithm to convert data to an unreadable code unless it is decrypted using a password. Provided only the sender and recipient of data know a password, the data will be protected against third parties even if the data is lost or intercepted. LSPs should use encryption to protect client files, especially sensitive information and information that is highly vulnerable. Encryption keys should be stored separately from the encrypted devices or media to ensure security.

Many operating systems and their supporting hardware can be configured to use encryption for all files or for files selected by the user.[26] Several different products are available to provide various levels of encryption capabilities. LSPs need to

26. *See supra* note 23. Encrypting files is a critical practice in many circumstances. LSPs should be mindful, however, that in some circumstances encryption may mask the introduction of malware into the network or obscure the theft of information. *See* KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON, Ch.14 (Crown Publish Group 2014); *see also* Karen Scarfone et. al., *Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices*, NIST (Nov. 2007), http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

be knowledgeable enough about the different encryption capabilities available to select the appropriate options for their needs. Third-party software for encryption is also readily available. Email applications can be set up to encrypt and automatically decrypt emails. Users simply need to exchange public keys and have their private key applied to decrypt messages; however, this key exchange process is burdensome within most standardized email environments and may lead to inconsistent application. Presently, there are third-party services that provide additional capabilities that make key exchange transparent and much easier to use. And mobile devices have encryption options—which can be managed through the device settings—that protect information when the device is locked.

Once information has been encrypted, it may then be securely transmitted through Secure File Transfer Protocol (SFTP), email, or cloud document management services. If information must be transmitted physically, the delivery method should reflect the sensitivity of the information. Highly sensitive information may need to be carried by a private courier or an LSP employee. The method of transport should be considered in avoiding unintended access due to the media being confiscated, lost, or stolen. If information is mailed, it should be sent in a manner so that it can be tracked at all times. Unencrypted sensitive information should never be placed in the mail or turned over to a courier for delivery. All too frequently, packages are lost, opened, or stolen in transit.

b. Mobile Devices

Mobile devices, such as laptops, phones, tablets, and PDAs are a practical necessity for LSPs. However, their portability and access to information also make them a target for information theft, even when they are "safely" located within an office environment. The primary tools for protecting the devices

from theft and intrusion consist of strong passwords, encryption, auto-locking defaults, device-tracing applications, and applications that allow the devices to be wiped remotely.

Through Mobile Device Management (MDM) the LSP can also remotely update mobile devices that are connected to any cellular network. It can thus install remote applications, configure settings, ensure security by updating and running malware detection software at pre-determined times (or on demand), enable device firewalls, disable public file sharing, avoid automatic connections to public WiFi, and even track and wipe lost or stolen devices.

c. Public WiFi

Additional security can be provided by deploying a strong employee-use policy with respect to mobile devices in public places. For example, personnel can be instructed to take special care when working with mobile devices in public by not connecting devices to public WiFi to access or transit client information. LSPs should set guidelines regarding the circumstances, if any, when an employee may use public WiFi to transmit client information.[27] Unencrypted client information

27. *See* Cal. State Bar Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. No. 2010-179 (2010), http://jolt.richmond.edu/wp-content/uploads/13-State-Bar-of-California-Opinion-2010-179-L0563533x7A34B.pdf. California requires attorneys to consider the following factors to determine appropriateness of a wireless communication:

> 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's

sent through public WiFi, including paid or free hotspots, can be easily compromised. Therefore, LSPs should clearly specify when use of public WiFi is and is not permitted and what additional protections are required.[28]

Policies should instruct employees to immediately notify the LSP if a mobile device is lost or stolen so the LSP may wipe or disable the device, as appropriate.

d. General External Use Security Considerations

When working outside controlled environments, employees should be instructed to use screen guards to prevent laptop screens from being viewed by the public, and to avoid discussing sensitive information in public. Employees also should be made aware of the vulnerabilities of blue tooth technology and potential for eavesdropping.

Policies should also instruct employees to immediately notify the LSP if a mobile device is lost or stolen and to subsequently wipe and disable the missing device.

e. BYOD and Personal Device Policies and Practices

Losing a client's business information, trade secrets, or privileged information can get an LSP in trouble with its client and perhaps with the state bar disciplinary counsel as well. Los-

---

instructions and circumstances, such as access by others to the client's devices and communications.

Id.

28. Options for additional protections may include use of virtual private networks (VPNs), which route data through a private connection. When possible, encrypted connections are also preferred through use of "https" addresses instead of "http" for websites and use of a Secure Sockets Layer (SSL) security protocol for applications.

ing sensitive client information that is subject to special regulatory restrictions, such as health related information, may generate regulatory involvement. Personal devices present one of the most significant risks to client information. These devices include home computers as well as mobile devices such as laptops, smartphones, and tablets. The best likely defense against the loss or theft of trade secrets, business information, privileged materials, and other sensitive information may be a strong and strictly enforced policy banning the use of personal devices to transact business or store such information. If an LSP permits its employees to use their personal devices to access private or confidential information, the LSP should consider taking the following steps to lessen the risk of using such devices:

- Allowing the use of *only* those devices that are specifically approved by the LSP's security professionals
- Requiring strong password and encryption policies
- Limiting the employee's ability to create or store LSP or client information directly on the device, by providing access only through secured portals to provider-protected networks. LSPs may also consider "sandboxing" mobile device applications that contain confidential information to shield provider applications from access by other applications or malware on the device.[29]
- Designating types of client information that should not be accessed, transmitted, or stored on a personal device. This may include infor-

29. Sandboxing effectively allows a device to host applications or data from multiple sources while blocking the flow of information or data from one part of the device to another.

mation that is subject to specific statutory protections, information that is otherwise highly sensitive, and information that clients have requested not be accessed by BYOD devices.

- Addressing employee home WiFi networks and devices used to create personal hotspots by requiring that these networks be secured with strong passwords that are not shared and are changed regularly

f. Travel Abroad

LSP personnel should avoid traveling overseas with client information or devices capable of accessing the LSP's IT systems, unless appropriate precautions and safeguards have been taken to account for increased security risks. Because this is a specialized area, LSPs might consider consulting or hiring third parties with expertise in network security involving traveling and transporting data outside the country.

LSPs should specifically address travel to high-risk geographic regions. It may not be possible or advisable for employees to directly access firm systems from high-risk areas. It may also not be advisable to allow employees to carry their normal devices or media with them into high-risk areas lest they be used to infiltrate the provider's systems. LSPs may also consider requiring employees to travel only with devices that do not contain sensitive information and adjusting default device settings on those devices. In addition, LSPs should consider whether WiFi connections are especially risky and adopt a policy of wiping devices both before traveling through foreign customs and before reconnecting them to the provider's network when they return home.

3. Security Among Third-Party Service Providers

The best information security program in the world can be nullified if the information is vested in the hands of another service provider who does not have adequate safeguards in place. For that reason alone, LSPs have a strong incentive to make sure the information they share with their experts, consultants, litigation support specialists, and other providers is well protected.

LSPs, like their clients and other businesses, increasingly rely on TPSPs to process, store, and manage information and IT systems. These TPSPs can include cloud storage providers, online human resource management companies, paper storage and destruction companies, eDiscovery service providers, enterprise-class online productivity services, Software as a Service (SAAS) cloud providers, and providers of outsourced IT staffing and services. Regardless of the TPSP or type of service offered, LSPs should consider following a set of best practices when engaging the services of such a TPSP on its own or on behalf of a client.

a. Understand the Type of Information the TPSP Will Handle

Before entering into an agreement with a TPSP, LSPs should carefully consider the type(s) of information that the TPSP will handle. For example, the following questions should be asked about the information to be accessed, processed, or stored by a TPSP:

- Will the TPSP handle client information, or only information belonging to the LSP itself, such as its own HR information?
- Will the TPSP handle PII, sensitive financial information, trade secrets, or privileged communications and materials?

- Are there any legal or regulatory restrictions imposed on the handling of the information? For example, does the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), or the Payment Card Industry Data Security Standard cover the information?
- Are there any contractual obligations related to the information? For example, will the TPSP handle client information covered by a HIPAA business associate agreement or EU Model Clauses agreement entered into by the LSP?

b. Ensure Compliance with Applicable Legal and Regulatory Requirements

LSPs should understand the legal and regulatory requirements applicable to the type of information that will be accessed, processed, or stored by the TPSP, and ensure that the TPSP is not only capable of meeting these requirements, but also is *contractually obligated* to do so.

c. Understand Geographic and Technical Risks Associated with the TPSP

LSPs should understand where their information will be stored and whether their information will be commingled with information belonging to other customers of the TPSP. TPSPs may store information in a variety of geographic locations, including overseas. The physical location of its information can

subject LSPs to litigation and regulatory oversight in the jurisdiction where information is stored.[30] LSPs must therefore understand and approve where its information will be stored. TPSPs may also commingle the information of their other customers. This is generally *not* a recommended arrangement for LSPs, because its information will be too sensitive to make the risks attendant with commingling acceptable. Thus, LSPs should avoid any arrangement in which information transferred to a TPSP will be commingled.

d. Conduct Due Diligence

A TPSP's viability is critical and LSPs should therefore obtain information about the TPSP's potential conflicts, and its financial stability under non-disclosure agreements. LSPs should also know the scope and policy limits of the TPSP's insurance coverage and ensure that the TPSP performs background checks on its employees and requires employees to sign confidentiality agreements.

e. Review and Approve the TPSP's Own Information Privacy and Security Policies Prior to Executing a Contract

No TPSP should be retained unless it has an appropriate information security and privacy policy. The TPSP's level of security and privacy protections should generally match or exceed those of the LSP. As a general matter, TPSPs should only be retained if they agree to meet an established standard, such

30. *See* Forward Food LLC v. Next Proteins Inc., 2008 WL 4602345 (Sup. Ct. N.Y. Oct. 15, 2008). The court found personal jurisdiction where a company's only contacts in New York consisted of a single visit, a few emails into the state, and a server located in the state containing the corporation's virtual data room.

as ISO 27001 and 27002. At a minimum, the LSP retaining a TPSP should consider contractually mandating each of the following:

1) Physical Security Controls

TPSPs must ensure the physical security of facilities housing sensitive information or from which such information can be accessed, including offices, offsite facilities, and locations of servers. Access to these facilities should be logged. These same recommendations apply to TPSPs that access, process, or store information belonging to the LSP or its clients.

2) Information Access Controls

TPSPs need to have appropriate preventative controls on accessing information, including, but not limited to, multi-factor authentication utilizing complex passwords, compartmentalization of information on the TPSP's systems, and access restricted to 'need to know' individuals.

3) Intrusion Detection Systems

TPSPs must employ an appropriate intrusion prevention system. If the information provided to the TPSP is highly sensitive and contains significant private or confidential information, LSPs should consider requiring the TPSP to employ an intrusion detection and monitoring system.

4) Encryption Procedures

Information sent to a TPSP should be encrypted while in transit to and from the TPSP. LSPs should also consider whether the sensitivity of the information warrants a requirement to encrypt information while it is stored ("at rest") by the TPSP.

5) Secure Disposition of Information

If the TPSP will store information for the LSP, it should agree that it will only use secure methods for disposing of that information or any hardware or media on which that information was stored.

f. Review and Approve the TPSP's Employee Training Program for Information Privacy and Security Prior to Executing a Contract

For both LSPs and TPSPs, proper employee and contractor training programs are essential to maintain information security and privacy. Before entering into an agreement with a TPSP, the LSP should inquire about the TPSP's employee and contractor training programs related to information security and privacy to ensure they are adequate. If the TPSP's training program is inadequate, the LSP should consider mandating the necessary improvements in the contract with the TPSP or finding another TPSP.

g. Ensure Appropriate Safeguards for Intellectual Property

Contracts with TPSPs should protect the intellectual property rights of the LSP and those of its clients. Use of a TPSP should not alter or adversely affect intellectual property rights.

h. Records Management

If a TPSP will store any information belonging to the LSP or its clients, the LSP should consider requiring the TPSP to adhere to the relevant existing records management and retention policies, except when doing so would frustrate the purpose of the TPSP's engagement, or when the TPSP is retained to provide an information archiving service.

i. Mandate Appropriate Information Disposition Upon Termination of the Relationship

The TPSP contract should require the TPSP to adhere to the records' policies of the client and to securely dispose of, or return, all the LSP's information in a useable form, in a timely manner, and upon termination of the relationship. Contractual clauses in which non-payment on the part of the LSP or its client justify refusal or delay in returning or providing access to information are generally not acceptable.[31]

j. Bankruptcy Protection

Careful consideration should be given to what will happen if the TPSP enters into bankruptcy. This scenario can be specifically addressed in the contract to ensure there is no dispute regarding ownership of the information or the media holding the information. Indeed, in certain situations, LSPs may wish to consider purchasing the physical media on which its information will be stored at the outset of the relationship, so there can be no question regarding the right or ability of the LSP to recover media-containing information.

k. Information Backup, Disaster Recovery, Access Continuity, and Incident Response

Before sending information to a TPSP, the LSP should be satisfied that the TPSP has adequate plans and equipment for disaster recovery, backup of the LSP's information, and response to incidents such as data breaches. The LSP should also ensure that the TPSP is contractually obligated to provide access

31. Indeed, even contractual commitments may not always protect a party from the misappropriation of highly sensitive private and confidential information. *See* Complaint, Glaxosmithkline LLC v. Discovery Works Legal, Inc., et al., No. 650210/2013 (Sup. Ct. New York County), filed Jan. 22, 2013.

to its information without excessive down time and will have an appropriate level of technical support available when needed.

l. Obligation to Assist in Discovery

In the event that information under the control of the LSP is in the possession or custody of the TPSP and becomes subject to a litigation hold or discovery obligation, a TPSP should be contractually required to render timely assistance in preserving and collecting information, as appropriate. Accordingly, the TPSP contract should include a clear benchmark for "timeliness" to avoid confusion regarding the degree of delay acceptable in implementing a litigation hold, and preserving and collecting the needed information. Similarly, the agreement should clearly set forth procedures to be followed by the TPSP if it directly receives a subpoena or other civil or law enforcement request for the LSP's information. In most circumstances, the TPSP should be required to immediately notify the LSP and cooperate fully with it in responding.[32]

m. Limitation on Sub-Contracting and Onward Transfers

A TPSP generally should not be permitted to allow a sub-contractor or other third party to access, process, or store the LSP's information without express prior approval for using the particular sub-contractor(s) or allowing the onward transfer(s) of information. Likewise, LSPs should not approve any such arrangements without first confirming that the sub-contractor(s) will be legally bound to comply with the same contractual provisions as the original TPSP.

32. In some situations involving requests from law enforcement authorities, immediate notification may be prohibited.

n. Accountability and Shared Liability

The contract between the LSP and the TPSP should consider proper incentives for compliance by imposing some form of liability on the TPSP for harm resulting from any failure to comply with its obligations under the agreement. LSPs should also consider requiring some form of indemnification of the LSP by the TPSP in the event of a data breach or other contract violation that exposes the LSP to liability. There are many potential mechanisms for imposing such liability, including liquidated damages or indemnification of the LSP by the TPSP.

o. Inspection and Monitoring

The contract should also give the LSP a right to audit the TPSP's compliance with its information, privacy, and security obligations, or to receive copies of the reports of an independent auditor. If the TPSP is concerned about giving the LSP access to its facilities or systems to test it for conflicts and security concerns, the agreement should allow for use of a mutually acceptable third-party "auditor." It is also critical that at least one thorough inspection actually be performed, and not merely permitted in theory. Additionally, parties should negotiate terms which contemplate updates to information privacy and security obligations as related technology and processes evolve.

p. Ensure Appropriate Access Controls for TPSP Personnel Given Access to LSP IT Systems

Where the contract calls for TPSP's personnel to have access of any sort to the LSP's own IT system, the LSP must make sure that it has appropriate safeguards in place. At a minimum, TPSP personnel who will have the ability to access the LSP's IT system should be subject to a background check, monitoring, and logging for unusual activity, and should have access to only the systems necessary to facilitate the purpose for which the

TPSP was engaged. The contract should also address the TPSP's responsibility and role with respect to providing notice and remediation in the event of any loss, theft, or breach of information caused by TPSP personnel.

D. Step 4: Establish Processes for Timely Disposition of Records and Information

LSPs should consider establishing policies, procedures, methods, and technologies suitable for deletion and destruction of client and third-party private and confidential information. Deletion of client information is necessary when directed by a client or triggered by the LSP's information retention policy. In general, information should be deleted when it is no longer needed. This means that LSPs should also ensure timely and thorough deletion of confidential information on devices of departing employees and on retired drives and devices during technology upgrades.

To ensure deletion policies are clearly understood by clients, when appropriate, LSPs should consider including a standard addendum to engagement letters that addresses the retention and disposition of client and third-party information. Such attachments should address standard policies and practices for the LSP handling the deletion of client information at the end of a matter, and provide instructions for the client to communicate its express wishes for the disposition of its information. Mid-matter deletion of certain unneeded documents may also be advisable, if a matter involves particularly sensitive information, and is not subject to a preservation obligation. If the provider plans to retain work product containing confidential client information after a matter has closed, because it has precedential value, the provider should clearly disclose its intention and obtain client consent. Standard policies and practices shared with clients about deletion of the client's files may address:

- whether the provider holds unique copies of documents potentially subject to a legal hold in other matters and whether the client would benefit from the LSP's retention of certain files from the closed matter;
- the level of sensitivity of the client's information held by the LSP;
- whether the client requires the LSP to retain certain documents, and whether other unnecessary files can be segregated and deleted;
- whether the client wants the LSP to send it a copy of the files to be deleted; and
- whether the client wants the LSP to keep copies of certain documents for safekeeping, and, if so, how those files will be stored.

The client retention letter, or a related addendum, should also address the disposition of information if a client becomes unavailable after the close of a matter. In that circumstance, the agreement might allow the client's information to be disposed of following a designated waiting period and in compliance with the LSP's applicable legal and ethical obligations.[33]

The waiting period should be set forth in the LSP's policies and made available to the client in the engagement letter. The addendum and a notice of the commencement of the applicable waiting period should be sent to the client after the matter closes. At the end of the applicable waiting period, the LSP

33. If the period was not determined by agreement between the LSP and the client, state rules may apply. *See, e.g.*, Ethics Op. 283, Disposition of Closed Client files, n. 9, DC Bar (July 1998), https://www.dcbar.org/bar-resources/legal-ethics/opinions/opinion283.cfm [hereinafter Ethics Opinion 283]; *see also* Materials on Client File Retention, ABA, http://www.americanbar.org/groups/professional_responsibility/services/ethicsearch/materials_on_client_file_retention.html (last visited June 3, 2015).

should direct that the client's information be disposed of in accordance with the LSP's legal and ethical obligations, unless the LSP becomes aware of a reason to continue to hold the information, e.g., it becomes potentially relevant to other proceedings involving the client. Policies should set forth procedures for a legal hold of the LSP's information in the event the LSP has an expectation that the files may be relevant in future litigation.

LSP policies should account for whether the LSP may have any legal or other obligation to retain files after a client's matter concludes and whether it may need to retain a copy of any files as a record of the work it did for the client. LSPs may therefore wish to create a deletion schedule where the LSP's work-product is held for a longer period than client-created or client-provided information. If the LSP determines it should keep its work product longer than its retention time, it should hold onto the work-product for only a reasonable period.

In instances where a client does not consent to retention of its confidential information after the close of a matter, the client file retained by the LSP may still contain work product that the LSP wishes to keep as precedent, form, or history (such as legal memoranda, pleading drafts, or case notes).[34] Under these circumstances, the LSP should "sanitize" those documents, removing confidential client information before storing the documents in the LSP's precedent bank or file repository.

Deletion of a client's confidential information should be comprehensive and involve all locations where the information resides.[35] Deletion will likely require efforts by the LSP's IT personnel and by the employees who accessed client information.

---

34. State bar rules and cases differ with regard to whether LSPs or clients own attorney work product. *See* Ethics Opinion 283, *supra* note 33 (raising but not deciding the issue).

35. "Deletion" methods and underlying hardware can differ in degrees of information recoverability. Physical shredding of the storage media

To the extent feasible, the LSP should confirm deletion from all potential locations, including document management systems, shared and private network storage, employee email, employee computers, electronic devices, external storage, backup files, and cloud servers. The LSP should also direct that the same steps be taken by any parties to whom they delivered client information, including opposing parties and TPSPs, as well as other LSPs. LSPs should deliver written confirmation to clients of having exercised reasonable diligence in the deletion of private or confidential information.

E. Step 5: Implement Training Program

People have unfortunate tendencies to lose things, speak at inopportune times, open strange emails, visit inappropriate websites, and so forth. Accordingly, LSPs need to train their owners and employees. Begin with teaching people about written information security and privacy policies that document and standardize the provider's practices for maintaining information security and confidentiality. Training should cover client information generally and identify categories of information that may require additional protection, identify applicable state and federal laws, and explain the nature of the client information held and any contractual obligations applicable to it.

---

is the most secure deletion of information but may be impractical. Therefore, more commonly acceptable standards of deletion include secure overwrite methods. Most drive electronics have built-in secure erase commands that can be activated with software and thoroughly erase the drive. LSPs may also consider using crypto-deletion where overwrite methods are insufficient or impractical, e.g., cloud services. Crypto-deletion involves encrypting information and destroying the encryption key rather than the information, rendering the information unusable. Deletion policies need to account not only for the LSP's technology infrastructure, but also regulations and requirements for specific types of information. For example, crypto-deletion may not be a valid solution for information if there is a strict requirement that the information must be scrubbed.

Information security and privacy policies clearly apply to all personnel who might handle PII or confidential client information. This includes the LSP's most senior people, its owners, managers, employees, contract staff, and other parties engaged by the LSP who can access private or confidential information.

The following elements are features that an LSP can consider including in its training program:

1. Mandatory for All Personnel

An LSP should consider making security training mandatory for all attorneys, paralegals, assistants, secretaries, contract staff, records staff, IT staff, and other personnel, regardless of whether such staff members will have access to sensitive information. Universal mandatory training is beneficial because the nature of IT systems and legal practice makes it highly likely that every employee will encounter private or confidential information at some point during their employment, and even those who do not could still be the source of a security breach that spreads beyond their own computer or office. It takes only one employee holding a door open for someone she does not recognize, or clicking on a link in an email message, to compromise an entire LSP's network.

2. Annual or Bi-Annual Frequency

The nature of security threats and tactics used by hackers and social engineers is constantly changing, as is the underlying technology. Accordingly, LSPs should consider sponsoring training on an annual basis. In addition to formal training on at least an annual basis, periodic reminders or updates might also be sent to all personnel reminding them of best practices and updating them on emerging threats. Besides keeping personnel informed, such regular reminders show that the LSP takes information privacy and security seriously and expects its employees

to do the same. Privacy and security training could also be mandatory for all new hires.

3. Accountability

There should be clear and meaningful consequences for personnel who fail to successfully complete training, or abide by the LSP's privacy and security policies. For example, LSPs who pay bonuses might want to consider reducing bonus compensation for employees who fail to complete training in a specified timeframe. Alternatively, they may wish to consider denying such employee access to the firm's network until training is completed.

4. Include Core Content

An ideal training program may include the following content:

a. General Background and a Clear Statement of Importance

Training programs should include a general overview or primer that provides a context for addressing information security and privacy issues. This primer should give examples that demonstrate the significance of these issues and the serious consequences that may result when information is inappropriately handled. These examples should reinforce the direct connection between the LSP's adherence to information and privacy principles and the LSP's reputation and success. This primer will therefore reinforce the serious damages the LSP may likely suffer if it—or its employees—violate laws surrounding information privacy/security or cause data breaches. These are both group and personal efforts, and training should convey that each employee is also personally responsible for maintaining the LSP's standards for privacy and security.

b. LSP Policies

Training should include all aspects of the LSP's information privacy and security policies, including policies regarding the use of social media and the use of mobile devices.

c. General Practices

In addition to explaining the LSP's own information privacy and security policies, training programs can include reasonable practices to maintain information security and privacy, such as those set forth in these Guidelines.

d. Applicable Ethical, Legal, and Regulatory Rules

Training programs should cover legal and regulatory rules applicable to the information held by the LSP.

e. Applicable Contractual Restrictions

If the LSP has access to information that is covered by contractual obligations, such as where a client has imposed additional information privacy or security restrictions on its information through a HIPAA business associate agreement, training should cover and highlight those additional requirements.

f. Role-Specific Requirements

In larger organizations where some employees, such as HR staff, may be exposed to a large amount of highly sensitive information covered by detailed regulatory requirements, additional role-specific training may be warranted for such employees.

g. Interactivity and Real World Scenarios

LSPs may wish to consider implementing training programs that present "real world" scenarios and prompt participants to indicate how they would respond under similar

conditions. For example, such training programs might provide examples of methods successfully employed in the past by hackers and social engineers to bypass security controls and obtain access to private or confidential information. In this way, the trainee can learn from past mistakes made by others and hopefully avoid repeating them.

5. Testing

In order to facilitate accountability and ensure mastery of the training material, LSP's training might also include a test that would be scored.[36] Failure to achieve a minimum score would then require the individual to continue or repeat the training until a satisfactory score was achieved.

6. Additional Messaging and Reminders

Larger organizations should consider supplementing formal training with posters, desk toys, and other aids to remind people on a regular basis of the importance of maintaining privacy and security over the LSP's information.

7. Training for Solo Practitioners and Small Offices

Receiving annual training meeting the above criteria is no less important for solo practitioners and their staff than it is for large law firms. However, it may be impractical for a solo practitioner or small law office to create an internal training program. Instead, such LSPs should consider using an accredited third-party organization; for example, by attending a conference, arranging for an in-house presentation, or employing a web-based solution.

36. This approach is similar to that already used in many training programs about sexual harassment and other HR issues.

F. Step 6: Preparing for the Worst

An information security program is not complete unless it includes provisions for the worst possible scenario. Technical problems and human mistakes are inevitable: a device will almost inevitably be lost or stolen, a critical server will irreparably crash, a social engineer will send a phishing email that someone will click on, or an intruder will breach the firewall and either damage the IT system or steal something, or both. An LSP should prepare and test a data breach response plan that anticipates common incidents.

This plan might consist of the following:

- Training all personnel to follow procedures for reporting and responding to potential information security breaches, including loss of devices or media, inadvertent transmission of information, or the interception or theft of information
- Identifying a person or a team to direct the LSP's response to a breach incident
- Creating a process for conducting a prompt investigation of a suspected breach, including assessing how and when the breach occurred, as well as what information sources have been compromised and what information is contained in those sources (If an investigation would likely require third-party forensic or IT experts, they should be identified beforehand and listed in the LSP's policy.)
- Depending on the risk profile of the LSP, running periodic "fire drills" or "table top" exercises to test the plan under various scenarios

(This will allow for the potential absence of employees who would ordinarily be critical to the successful implementation of the plan.)

- Developing procedures to mitigate damage when a breach is ongoing, bearing in mind that unplugging the affected computer may not necessarily be the best approach to defeat a sophisticated attack or to preserve important evidence (Indeed, in some instances the "obvious" source of the intrusion may only be a decoy meant to distract the security team from the real assault on the LSP's systems.)
- Contingency plans for providing notice to the owners of compromised information, including clients and other interested parties after a breach or loss is confirmed
- Developing procedures to revise and adjust policies after an unauthorized disclosure, loss, or theft breach to avoid future occurrences
- Implementing a system to receive news and updates of reported breaches outside of the LSP, which may affect the LSP's information security[37]
- Notifying appropriate law enforcement authorities and insurers
- Abiding by applicable breach notification regulations

---

37. *See*, *e.g.*, U.S. Department of Homeland Security, US-CERT, https://www.us-cert.gov. In the future, LSPs may also create an anonymous repository through which hacking and threat information could be shared. *See* Matthew Goldstein, *Wall St. and Law Firms Plan Cooperative Body to Bolster Online Security*, N.Y. TIMES, Feb. 23, 2015, *available at* http://www.nytimes.com/2015/02/24/business/dealbook/wall-st-and-law-firms-weigh-cooperation-on-cybersecurity.html.

V. CONCLUSION

LSPs and TPSPs have the responsibility to take reasonable steps to protect private and confidential information, a responsibility that is grounded in the ethics rules applicable to lawyers as well as in federal, state, and common law rules. In some situations, a duty may also arise under the laws of foreign nations. This Commentary is intended to help LSPs assess security risks and provides guidelines for implementing privacy and information security policies.

APPENDIX A: PRIVACY AND SECURITY IN THE HEALTH CARE INDUSTRY

Privacy and security requirements are not new to the health care industry. LSPs who work with health information are subject to rules governing privacy and security as defined in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Clinical and Economic Clinical Health (HITECH). These laws regulate the disclosure of personal information by health care providers and those who provide services to the health care providers, including lawyers. Both HIPAA and HITECH directly affect LSPs who perform work for those covered by the laws and they potentially provide guidance to other LSPs as well. Thus, among other things, HIPAA:

- provides privacy protection for protected health information (PHI);
- mandates security requirements;
- addresses data breaches/breach notification requirements;
- mandates notice of privacy practices;
- governs sales of PHI and regulates sharing of PHI;
- requires consent and bars certain disclosures; and
- mandates Business Associate Agreements for entities that create, receive, store, maintain, or transmit PHI (Business Associates are responsible for their subcontractors), including law firms and other LSPs.

With minor exceptions, a Business Associate (BA) is a person or entity who performs work involving access to PHI on

behalf of, or provides certain services to, a covered entity.[38] Similarly, under the HITECH Act, LSPs and vendors may be considered BAs. HITECH provides that BAs are subject to the HIPAA Security and Privacy rules that apply to electronically stored PHI (e-PHI).

This means that LSPs who possess or work with HIPAA-protected information must impose protections into three safeguard categories: physical safeguards (e.g., physical measures, policies, and procedures to protect the information systems and buildings from natural and environmental hazards, and unauthorized intrusions); administrative safeguards (e.g., developing information security policies and procedures, appointing a security officer, sanctioning violations, and providing regular training);[39] and technical safeguards (e.g., policies and procedures governing access and disposal of electronic PHI).[40]

In addition, the HITECH breach notification procedures require giving notice to every person affected by any breach involving PHI. Such notices must be issued within sixty days of the discovery of the breach, and if the breach involves more than 500 people, the Department of Health and Human Services (HHS) must be notified. Similarly, the regulations require a

---

38. *See* 45 C.F.R. § 160.103, *available at* http://www.hipaasurvivalguide.com/hipaa-regulations/160-103.php; *Health Information Privacy*, *Business Associates*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES (last revised Apr. 3, 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.

39. *Summary of HIPAA Security Rule*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html (last visited September 10, 2015).

40. *HIPAA Security Series*, *Technical Safeguards*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (last visited October 9, 2015).

statement to the media if the breach involves more than 500 individuals.[41] These regulations directly affect those who perform legal services for entities such as hospitals, insurers, or other businesses in the medical industry.

The Administrative Simplification provisions of HIPAA establish a baseline level of standards and requirements for the transmission and handling of health information. The provisions are intended to improve the efficiency and effectiveness of the health care system while protecting patient privacy, and they can be adopted to provide useful benchmarks for LSPs who work outside the HIPAA arena.

The BA concept can have useful application to sensitive information beyond HIPAA.[42] Practical experiences that have been gained in the health care industry provide useful guidance for LSPs seeking to protect client information of any type when sharing it with third parties. This is especially true with respect to BA contracts that ensure PHI will be safeguarded. The BA contract clarifies and limits the permissible uses and disclosures of PHI by the business associate. A BA may use or disclose protected health information only as permitted or required by its business associate contract or as required by law.

Under HIPAA, a BA is directly liable and subject to civil, and possibly criminal, penalties for improperly using and/or disclosing PHI. A BA is also directly liable and subject to civil

---

41. 45 C.F.R. § 164.408, *Health Information Privacy*, *Instructions for Submitting a Notice of Breach to the Secretary*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

42. *See* Iliana Peters, HHS Office for Civil Rights, *Lessons Learned From Recent HIPAA Breaches*, presented at Safeguarding Health Information: Building Assurance through HIPAA Security, Washington, DC (September 3, 2013), http://csrc.nist.gov/news_events/hipaa-2015/presentations/2-7-peters-update-hipaa-compli.pdf.

penalties for failing to safeguard electronic PHI in accordance with the HIPAA Security Rule. Although such statutory liability is not usually available with ordinary service contracts into which LSPs enter, indemnification clauses are, of course, an option. See discussion at Part IV.C.3.n., *supra*. The BA guidance provides a thorough framework to implement similar contracts to help protect non-HIPAA regulated information.

Accordingly, LSPs that handle protected information must enter into BA agreements with their covered clients and establish appropriate administrative safeguards for the protection of the confidential records. The written BA agreement must also provide for the destruction or disposition of all protected information at the end of any engagement. In the event of a breach, which is defined as the "impermissible acquisition, access, use, or disclosure of PHI (paper or electronic), which compromises the security or privacy of the PHI,"[43] the LSP must follow HHS[44] or Federal Trade Commission (FTC)[45] Breach Notification procedures, as appropriate. Application of the BA safeguards to all sensitive information enhances the defensibility of security measures and predictability should anything go wrong.

The Health and Human Services (HHS) Office of Civil Rights (OCR) is responsible for enforcement of the HIPAA Privacy and Security Rules and the confidentiality provisions of

---

43. *Id*.

44. *Health Information Privacy, Breach Notification Rule*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule (last visited June 3, 2015).

45. *Complying with the FTC's Health Breach Notification Rule*, FEDERAL TRADE COMMISSION (Apr. 2010), https://www.ftc.gov/system/files/documents/plain-language/bus56-complying-ftcs-health-breach-notification-rule.pdf.

the Patient Safety Act and Rule. The OCR maintains responsibility for review of entities such as hospitals, pharmacies, health insurance companies, managed health care plans, employer group health plans, and government health plans such as Medicare and Medicaid. Like the OCR, the FTC also plays an important role in the oversight and enforcement of the HIPAA Privacy and Security Rules.

HIPAA established for the first time a set of standards to address the use and disclosure of individually identifiable health information. In coordination with OCR, the FTC promulgated its Health Breach Notification Rules.[46] The FTC breach notification requirements implements § 13402 of the HITECH Act and requires HIPAA-covered entities and their BAs to provide notification following a breach of unsecured, protected, health information. Similar breach notification provisions are implemented and enforced by the FTC for personal health records, pursuant to § 13407 of the HITECH Act (e.g., the FTC Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (2014)).

Outside the healthcare context, the U.S. Commodity Futures Trading Commission (CFTC) Staff Advisory No. 14-21 (Feb. 26, 2014) contains similar useful guidance regarding best practices. Under the HITECH Act, State Attorneys General also maintain legal authority to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules. Toward that end, the OCR developed HIPAA Enforcement Training to help State Attorneys General and their staff use their new authority to enforce the HIPAA Privacy and Security Rules.[47] This guidance can also be useful to

46. *Id*.

47. *Health Information Privacy*, *HIPAA Enforcement Training for State Attorneys General*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES,

LSPs in understanding the process by which State Attorneys General may review and investigate HIPPA-related complaints.

The HIPAA privacy rule governs how a legal service provider is expected to handle the use or disclosure of PHI. In general, when State law is "more stringent,"[48] then State law will supersede the HIPAA privacy rule. Conversely, if a HIPAA state law is less stringent, then federal HIPAA rules apply. State law is considered to be "more stringent" than the HIPAA Privacy Rule if it relates to the privacy of individually identifiable health information and provides either greater privacy protections for individuals' PHI, or greater rights to individuals with respect to that information, than does the Privacy Rule.[49] The definition of the "more stringent" standard is set out at 45 C.F.R. § 160.202.

Finally, the National Institute of Standards (NIST) in collaboration with the National Cybersecurity Center of Excellence (NCCoE) has developed and released a first draft of a cybersecurity practice guide to help organizations of all kinds and sizes deploy technical standards that promote the secure collection, storage, processing, and transmission of PHI contained on mobile devices. Organizations can use some or all of the NCCoE guide to help them implement health care industry standards

---

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html (last visited September 10, 2015).

48. For a definition of what is considered to be a 'more stringent' HIPAA state standard, *see* 45 C.F.R. § 160.202, *available at* http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec160-203.pdf (last visited June 3, 2015).

49. *Health Information Privacy*, *State Attorneys General*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/ (last visited June 3, 2015).

and best practices, as well as those in the NIST Framework for Improving Critical Infrastructure Cybersecurity.[50]

50. The draft guide is available to download in sections from NIST *at* https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices:

SP 1800-1a: Executive Summary

SP 1800-1b: Approach, Architecture, and Security Characteristics

SP 1800-1c: How-To Guide

SP 1800-1d: Standards and Controls Mapping

SP 1800-1e: Risk Assessment and Outcomes

These standards provide valuable guidance to LSPs who are working to establish healthcare eDiscovery standards for the collection, production, and transmission of PHI.

APPENDIX B: PRIVACY AND SECURITY IN THE FINANCIAL SERVICES INDUSTRY

A. Financial Services Defined

Law firms and other LSPs in the U.S. also face a complex blend of security and privacy regulations and guidelines relating to financial information collected or used by financial institutions. The term "financial institution" is broad and potentially includes not only banks and brokerages but also check-cashing businesses, data processors, mortgage brokers, non-bank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers. The common denominator here is the range and sensitivity of personal data typically collected or held by these financial institutions, which includes names, addresses, phone numbers, bank and credit card accounts, income and credit histories, and social security numbers.

Much of the regulatory activity surrounding financial services stems from the individual and systemic importance, and significant risks associated with the handling, of such information. The wide range of potential actors, the extensive access by many LSPs to confidential financial information, and specific references to service providers in the relevant rules, have led to elevated regulatory scrutiny of the financial services sector and raised its litigation risk profile.

B. LSPs Are Particularly Vulnerable to Loss of Confidential Information

LSPs are commonly entrusted with highly sensitive and valuable financial information, both directly by their clients and because of their work with other parties. With such access comes a high level of scrutiny and risk. Wrongdoers often consider LSPs to be weak links in the information security chain and

therefore are easy targets. According to Mary Galligan, the former head of the cyber division in the New York City office of the U.S. Federal Bureau of Investigation, "as financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it's a much, much easier quarry."[51] Similarly, Richard Vallanueva, special agent for the United States Secret Service Electronic Crimes Task Force, states that hackers are increasingly targeting law firm escrow accounts as the path of least resistance. Mandiant, a specialized security firm, estimated in 2012 that eighty major U.S. firms were hacked each year.[52] That number may, in fact, be too low. While law firms are reticent to make public such breaches of security, Bloomberg reported in 2012 on the deliberate infiltration by China-based hackers of the computer networks of seven different Canadian law firms, as well as the Canadian Finance Ministry and Treasury Board.[53] The hackers stole important information in what appears to have been an attempt to derail a $40 billion acquisition of a potash producer by an Australian mining company.[54]

Confidential client information held by law firms has also received attention from governmental actors. Documents revealed by Edward J. Snowden showed that, in the course of representing the government of Indonesia in trade negotiations with the U.S., at least one global law firm's privileged client communications were intercepted by an Australian governmental security agency, which passed them on to the U.S. National

51. Michael A. Riley & Sophia Pearson, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, BLOOMBERG TECHNOLOGY (Jan. 31, 2012), http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.

52. *Id*.

53. *Id*.

54. *Id*.

Security Agency (NSA).[55] According to the *New York Times* article, "[o]ther documents obtained from Mr. Snowden reveal that the NSA shares reports from its surveillance widely among civilian agencies."[56]

Financial institutions have taken notice, and they are increasingly subjecting law firms to exacting data security and handling requirements and examination. These standards may vary slightly according to the nature of the information received, but baseline compliance on a number of security and confidentiality measures is growing as a measure of continued relationship success. Accordingly, whether viewed from a legal, business, or ethical standpoint, law firms need to consider the wide variety of threats to the security of the information they possess and take reasonable steps to safeguard their systems and clients' information from accidental or intentional breach. In particular, where the firm works with financial institutions, these issues should be considered early in the relationship because later scrambling efforts may be insufficient for a continued client relationship.

1. GLBA Privacy Rule

There is a growing body of law and regulation governing financial services information security and privacy. Foremost is the Financial Services Modernization Act of 1999 (the "Gramm-Leach-Bliley Act," or GLBA). The GLBA requires financial institutions to implement privacy and security protections to ensure the protection of consumers' information. In a form and structure similar to HIPAA, the GLBA created separate but interdependent obligations designed to minimize the risk associated

55. *See* James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES, Feb. 15, 2014, *available at* http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html.

56. *Id*.

with third-party access and use of financial data. The GLBA provides for the implementation of standards to limit the purposeful disclosure of and protection against unauthorized access to consumers' "nonpublic personal information." The privacy rule focuses on notification, opt-out rights, and limits on use and disclosure. The security rule addresses security risks. In 2003, the FTC created separate rules for privacy and security to require financial institutions to "explain their information-sharing practices to their customers and to safeguard sensitive data."[57] The FTC and its regulatory cousins, the FRB, OCC, FDIC, SEC, NCUA, OTS, and CFTC[58] collaborated to develop, through consumer testing, "privacy notices that consumers can understand

57. *Gramm-Leach-Bliley Act*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited June 3, 2015).

58. The Federal Reserve Board (FRB) is the governing body of the Federal Reserve System. *See* http://www.federalreserve.gov/. Office of the Comptroller of the Currency (OCC) "charters, regulates, and supervises all national banks and federal savings associations as well as federal branches and agencies of foreign banks." *See* http://www.occ.gov/. The Federal Deposit Insurance Corporation (FDIC) provides deposit insurance for depositors. *See* https://www.fdic.gov/. The U.S. Securities and Exchange Commission (SEC) acts to "protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation." *See* http://www.sec.gov/. The National Credit Union Administration (NCUA) regulates, charters, and supervises federal credit unions. *See* http://www.ncua.gov/. The Office of Thrift Supervision (OTS) was formerly tasked with providing support for federally and state-chartered savings banks and savings and loans associations; OTS ceased operations on October 19, 2011. The U.S. Commodity Futures Trading Commission (CFTC) operates to "protect market participants and the public from fraud, manipulation, abusive practices and systemic risk related to derivatives—both futures and swaps—and to foster transparent, open, competitive and financially sound markets" by policing the derivatives markets. *See* http://www.cftc.gov/index.htm.

and use to compare financial institutions' information collection and sharing practices."[59]

The GLBA distinguishes between consumers and customers, and imposes different obligations to provide privacy notifications to each. A consumer is an "individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons." In contrast, a "customer is a consumer with a continuing relationship with a financial institution." This distinction is important, because only customers are entitled to receive a financial institution's privacy notice automatically, while consumers may receive a privacy notice from a financial institution only if, and when, a company shares the consumer's information with unaffiliated organizations.

2. GLBA Security or Safeguards Rule

The security or "Safeguards" Rule applies to those "significantly engaged in providing financial products or services to consumers, including check-cashing businesses, data processors, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers."[60]

---

59. *Financial Privacy Rule: Interagency Notice Research Project*, FEDERAL TRADE COMMISSION (Apr. 15, 2010), http://www.business.ftc.gov/documents/0496-financial-privacy-rule-interagency-notice-research-project; for an example of congressional actions to tighten up security and breach notification laws, *see U.S. Congress Ready To Enact Data Security And Breach Notification Rules After Recent Consumer Data Breaches*, JONES DAY (Feb. 20, 2014), http://www.jonesday.com/us-congress-ready-to-enact-data-security-and-breach-notification-rules-after-recent-consumer-data-breaches-02-14-2014.

60. *See Safeguarding Customers' Personal Information: A Requirement for Financial Institutions*, FEDERAL TRADE COMMISSION (May 2002), https://www.ftc.gov/system/files/documents/plain-language/alt115-safeguarding-customers-personal-information-requirement-financial-institutions.pdf.

The FTC requires a written information security plan and delineates five core program components for safeguarding information, with the actual design and ultimate implementation dependent on, and appropriate to, variations in size, complexity, nature and scope of activities, and the sensitivity of customer information. Similar to HIPAA's Business Associate relationship, the Safeguards Rule explicitly requires financial institutions to include security safeguard language in their contractual relationships with service providers, including law firms. Covered financial institutions must:

- designate the employee or employees to coordinate the safeguards;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks;
- design a safeguards program, and detail the plans to monitor it;
- select appropriate service providers and require them (by contract) to implement the safeguards; and
- evaluate the program and explain adjustments in light of changes to its business arrangements or the results of its security tests.[61]

61. *Safeguarding Customers' Personal Information: A Requirement for Financial Institutions*, FEDERAL TRADE COMMISSION (May 2002), https://www.ftc.gov/system/files/documents/plain-language/alt115-safeguarding-customers-personal-information-requirement-financial-institutions.pdf (last visited June 3, 2015) (citing to FTC Safeguards Rule 16 C.F.R. Part 314 and http://www.nacua.org/nacualert/docs/GrammLeachBliley_Act/16_CFR_314.pdf).

While the FTC explicitly allows flexible implementation of the rules and programs, it also provides both general and specific guidance to financial institutions. Considerations proposed by the FTC include, but are not limited to, the following:

- Employee training and management
- Encryption and password protocols
- Robust preventative and reactive auditing for data at rest, in transit, and during use
- Individual, network, and Web-based programs and controls
- Proper and secure disposition of confidential information[62]

The FTC has also issued a variety of publications designed to provide more granularity around its general safeguards.[63]

In much the same fashion as HIPAA, LSPs in contact with information covered by GLBA must implement administrative, technical, and physical safeguards that are documented and audited. These "umbrella" categories do not create a bright line of "reasonableness" for assessing or auditing information security and privacy safeguards, although they do provide sufficient detail within a flexible framework—tailored to the nature of the information at issue—to guide LSPs within the scope of the GLBA.

---

62. *Financial Institutions and Customer Information: Complying with the Safeguards*, FEDERAL TRADE COMMISSION (Apr. 2006), http://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

63. *See*, e.*g.*, *Protecting Personal Information, A Guide for Business*, FEDERAL TRADE COMMISSION (Nov. 2011), http://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

3. Enforcement

Regulatory enforcement of these regulations and others relating to financial sector security and the privacy of consumer information vary greatly depending on the nature and size of the institution. The FTC has authority to enforce the law with respect to "financial institutions" that are not covered by the federal banking agencies, the OCC, the SEC, the CFPB, and the FDIC. The FTC uses its FTC Act Section 5 authority when enforcing the Safeguard Rule of the Gramm-Leach-Bliley Act to determine whether a company's information security measures were reasonable and appropriate.[64] The OCC, SEC, CFPB, FDIC, and various state regulatory agencies, also have enforcement capabilities in this area.

The authority to regulate and enforce information and security protections for LSPs is both express and implied. On April 13, 2012, the CFPB issued a bulletin defining its enforcement power, with a particular emphasis on the impact of service providers to financial institutions. The bulletin noted CFPB's goal to ensure compliance with "Federal consumer financial law," including GLBA and its implementing regulations, the Privacy Rule and the Safeguards Rule, noting that legal responsibility for the conduct of service providers in addressing these rules "may lie with the supervised bank . . . as well as with the supervised service provider." The CFPB expects supervised banks to have an effective process for managing the risk of their service providers, including reviewing and monitoring the service providers' policies, procedures, internal controls, and training materials.

64. Jennifer Woods, *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5*, ABA, http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html (last visited June 3, 2015).

The OCC also addressed third-party risk on October 30, 2013, highlighting the following:[65]

- Risk management should be commensurate with the level of risk and complexity of its third-party relationships.
- Regulated entities should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the third-party business relationship includes:
    1. plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party;
    2. proper due diligence in selecting the third party;
    3. written contracts that outline the rights and responsibilities of all parties;
    4. ongoing monitoring of the third party's activities and performance;
    5. contingency plans for terminating the relationship in an effective manner;
    6. clear roles and responsibilities for overseeing and managing the relationship and risk-management process;
    7. documentation and reporting that facilitates oversight, accountability, monitoring, and risk management; and

65. OCC BULLETIN 2013-29, Third-Party Relationships, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Oct. 30, 2013), http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

8. independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

Shortly after addressing third-party risks, the OCC developed a set of "heightened expectations" to strengthen governance and risk-management practices at large banks and federal savings institutions to enhance the agencies' supervision of those institutions. On January 16, 2014, the OCC issued proposed guidelines pursuant to section 39 of the Federal Deposit Insurance Act that enhance and formalize these expectations. These expectations include:

- roles and responsibilities definition relating to the three lines of defense; and[66]
- strategic plans from critical stakeholders on risk management Risk Appetite Statement.

---

66. *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of 12 CFR Parts 30 and 170*, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Jan. 10, 2014), http://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-4a.pdf:

> i) The first line is provided by the business units—comprising the business units, support functions, and embedded operational risk staff.
>
> ii) The second line is provided by the risk management function—comprising the operational risk management function and the compliance functions. To qualify in this category, the risk management function usually demonstrates the qualities detailed in the operational risk management function section.
>
> iii) The third line is the audit function. A number of TSA firms have outsourced their audit function. The underlying arrangements and effectiveness of an outsourced audit function should be assessed for its suitability.

The FDIC has also issued its own guidelines ("Interagency Guidelines") for information security standards, as required by Section 39 of the FDIC Act and Section 501 and 505(b) of the GLBA. These guidelines address administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. The Security Guidelines set forth specific requirements that apply to a financial institution's arrangements with service providers.

An institution must:

- exercise appropriate due diligence in selecting its service providers;
- require its service providers by contract to implement appropriate measures designed to meet the objectives of the Security Guidelines; and
- where indicated by its risk assessment, monitor its service providers to confirm that they have satisfied their obligations under the contract described above.[67]

A service provider is *any* party that is permitted access to a financial institution's customer information through the provision of services directly to the institution. Examples of service providers include a person or corporation that tests computer systems or processes customers' transactions on the institution's behalf, document-shredding firms, transactional Internet banking service providers, and computer network management firms. LSPs are generally engaged directly by the institution and

67. *See Interagency Guidelines Establishing Information Security Standards*, FDIC (Apr. 20, 2014), https://www.fdic.gov/regulations/laws/rules/2000–8660.html; *see also Interagency Guidelines Establishing Information Security Standards*, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, n. 2 (Aug. 2, 2013), http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm#fn2.

so would likely fall within the definition of service provider and, therefore, assume the obligation and expectation of compliance with the detailed FDIC security guidelines.[68] Another potential benchmark for reasonableness of which LSPs should be aware is a separate initiative led by large financial institutions to standardize third-party risk assessments.

The Shared Assessments Program is rooted in ISO 27001 and uses a Standard Information Gathering program (SIG) to collect details about a service provider's controls (people, process, and procedures), and is supported by a verification protocol to ensure accurate assessment and reporting. The Shared Assessments was created by the Bank of America Corporation, The Bank of New York Mellon, Citibank, JPMorgan Chase & Company, U.S. Bankcorp, and Wells Fargo & Company in collaboration with leading service providers and the Big Four accounting firms to help financial services companies assess service providers. In 2014, the Shared Assessments issued results of its Vendor Risk Management Survey, with a third of the responses coming from financial institutions. The survey was based on the following eight vendor risk categories:

1. Program Governance
2. Policies Standards Procedures
3. Contracts
4. Vendor Risk Identification and Analysis

68. On a related note, agency-reporting requirements on privacy breaches are now accompanied by disclosure obligations for cybersecurity risks and cyber incidents. On October 13, 2011, the SEC Division of Corporation Finance issued guidance on disclosure obligations relating to cybersecurity risks and cyber incidents. The guidance applies to domestic and non-U.S. SEC registrants to assist registrants in preparing disclosures under the Securities Act of 1933 and the Securities Exchange Act of 1934. *CF Disclosure Guidance: Topic No. 2*, U.S. SECURITIES AND EXCHANGE COMMISSION (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

5. Skills and Expertise
6. Communication and Information Sharing
7. Tools, Measurement, and Analysis
8. Monitoring and Review[69]

CONCLUSION

Both the health care services and financial services industries are subject to laws and regulations that: (1) impose security standards on industry members; (2) require special service contracts between those who collect information directly from consumers and those who provide services to them; (3) require notification to consumers when security lapses result in the loss of information pertaining to a non-*de minimis* number of consumers; and (4) subject those who lose data to potential legal liability. Keeping abreast of the best and current practices in these industries may be informative to the LSPs in establishing processes and programs for not only dealing with information obtained from those industries, but also for treating privacy-related and other confidential information obtained from others.

69. Shared Assessments, https://www.sharedassessments.org/ (last visited June 3, 2015).