

KIRKLAND & ELLIS LLP

Safeguarding Confidentiality: Ensuring Your Technology, Policies and Practices Protect Sensitive Client and Firm Information

by Ann Ostrander, Senior Director, Firmwide Loss Prevention, Kirkland & Ellis LLP

Kirkland & Ellis LLP is a 1,500-attorney law firm representing global clients in complex intellectual property and technology matters, litigation and dispute resolution/arbitration, corporate and tax, restructuring and real estate. The firm has a dedicated loss prevention group, charged with mitigating risk and protecting the organization's assets and reputation. This group works to classify a variety of risks tied to both firm and client interests, and to coordinate efforts to prioritize and mitigate them.

Confidentiality management has always been an important priority for our firm. And in recent years, several factors have contributed to the increasing profile of this issue. The first is the continued growth of electronic information, largely driven by the proliferation of technology to create, copy, store and share this information. From a loss prevention perspective, law firms bear significant responsibility in ensuring that client information, attorney work product and relevant records are handled properly at all stages of the matter lifecycle. In this context, the confidentiality policies, practices and controls that make certain only authorized individuals can view sensitive information are just one part of this lifecycle, but they are an important one.

The second set of factors raising the profile of this issue include evolving and expanding industry rules, government regulations, client requirements and case law. While each has a different impact on confidentiality, a common thread unites all of these factors – the world is paying closer attention to law firm practices.

Anecdotally, this attention may take the form of a client that's concerned about how broadly its sensitive internal information might be accessible within the firm, or by a State Bar Association updating screening rules to acknowledge that information flows differently within a large, global, 800-attorney firm compared to a small, regional, 8-attorney firm. As we'll explore in greater detail, these anecdotes are the result of an overall trend towards more detailed and explicit expectations from external influencers and regulators about information accessibility and confidentiality practices within law firms.

To respond, risk-focused organizations are pursuing more stringent internal confidentiality measures and taking steps that enable them to document and verify compliance. Thankfully, updating firm approaches to confidentiality management does not have to be a painful endeavor that adds undue overhead and inconvenience. But to successfully manage this growing risk, it is important to take some basic steps to revise firm policies, revisit internal training procedures and leverage technology.

What is Confidentiality?

While confidentiality has a different meaning in the context of a non-client, third-party attempting to obtain access to protected or privileged information, in the context of internal information, the core of confidentiality boils down to three simple questions:

- Who has access to specific information?
- Does anyone have access to that information who should not?
- Can the firm demonstrate compliance with its own policies and applicable rules if required to do so?

continued

When is Confidentiality Required?

The firm has an affirmative duty to protect client information from unwarranted external disclosure. But even inside the firm, access to internal information must be more closely controlled for reasons including:

- **Client Requirements** – Increasingly, clients want to restrict who within the firm is able to access their sensitive business information. Examples might include IP matters, strategic or financial matters of significant import or implication, or high-profile entities or individuals with sensitivities about the potential for public disclosure. These clients may stipulate protective measures that run contrary to standard firm information management practices. Such measures may include “defined matter team only” access and other tracking and reporting obligations.
- **Ethical Screens** – Ethical screens are access restrictions that are frequently created when a lateral hire with a past adversarial relationship with an existing client joins the firm. The effectiveness of screens often depend on the nature of the previous relationship, the level of matter involvement and applicable jurisdictional rules. In some instances, client waivers are required (and clients have been known to require the firm to detail specific confidentiality enforcement measures before consenting). In other scenarios, unilateral screening may be permitted. Importantly, as opposed to client-driven confidentiality, in screening scenarios, information related to the matter may still be made accessible generally within the firm. Only the restricted party needs to be prevented from access to materials or interacting with identified matter teams.
- **Government Regulations** – Specific government laws and regulations extend to client information held by law firms. In the United States, rules like HIPAA extend to personally identified health-related information. Firms practicing internationally may also be subject to a variety of local rules. In some instances, international rules include mandatory creation and tracking of an audit trail throughout the life of the matter.

Additionally, the firm itself likely has private information which should be subject to confidentiality protections. Such information may be related to legal matters the firm or its partners are engaged in (e.g. litigation or other business matters), human resources-related materials or other private information related to the internal business of the firm. In these cases the organization has an interest in preventing associates and staff from accessing this information, whether on purpose or accidentally through the use of tools such as enterprise search technologies.

How Confidentiality Is Often Managed (And Why Traditional Methods Often Fall Short)

Traditionally, firms set up ethical screens by distributing memoranda and relying on the professional diligence of attorneys and staff. Additionally, and in response to screens or specific client confidentiality requirements, firms may also manually create access limitations within their document management application or set up separate repositories for restricted matters.

Unfortunately, legacy approaches like these may fall short for several reasons. Approaches that rely on notification and individual responsibility create the risk of accident and inadvertent access, especially at organizations using software search tools which may unearth unintended results. Manual approaches also create overhead and increase the risk that restrictions may fall out of date over time. For example, an attorney unaware of a restriction may request the firm’s IT help desk to grant access to a confidential document, and the help desk may unknowingly comply. Or an attorney may be asked to help on a confidential matter but not notified about the screening policies. Importantly, as these examples illustrate, problems need not occur due to deliberate wrongdoing. Rather, accidents and unintended mistakes are, in most cases, the bigger concern.

Closing the Gaps – Understanding and Responding to Confidentiality Rules, Requirements and Trends

When revising screening practices, firms should first look to specific rules of professional responsibility and case law in their jurisdictions. However, as confidentiality applies in situations beyond traditional conflicts-related screening, a broader understanding of how the courts, peer states and the industry as a whole evaluate the suitability of confidentiality is important. Indeed, as standards continue to evolve, it’s common for different jurisdictions and stakeholders to observe and influence one another.

Legal industry trends point to a growing acceptance of unilateral screening as a means to address lateral conflicts. Judges are looking at guidance such as the recently-modified ABA Model Rule 1.10, which allows lateral screening, without consent, subject to new enforcement and notification requirements. To date, twenty-four states have adopted similar

screening provisions. The ABA amendment sets a more stringent standard than most state rules, requiring proactive client notification that includes a description of screening measures and regular compliance acknowledgements by attorneys. Recent cases that highlight the continuing refinement and development of screening enforcement standards include:

- **Norfolk Southern Railway v. Reading Blue Mountain et al.** [397 F. Supp. 2d 551 (M.D. PA. 2005)] – Which holds that a screen must be demonstrated to be “effective” in order to withstand challenge.
- **Rockaway Bedding, Inc., Debtor, U.S. Bankruptcy Ct.** [42-6-7393 (Steckroth, U.S.B.J.) 2007] – The court, denying a disqualification motion, highlighted the use of “an electronic” ethical wall to isolate professionals as key criteria demonstrating effectiveness. The use of security software was similarly cited in **Papyrus Technology Corp. v. New York Stock Exchange** [325 F. Supp. 2d 270 (S.D.N.Y. 2004)].
- **Tucker v. Rossmiller** [560 F. Supp. 2d 834 (W.D. Wis. 2008)] – Which holds that screening and confidentiality processes need to be a “formal mechanism” and that ad hoc responses are insufficient even they result in no breaches.
- **Chinese Automobile Distributors of America LLC v. Bricklin** [2009 U.S. Dist. Lexis 2647] – A recently-issued decision which further emphasizes the need for speed and stresses the standard of enforcement: “...the firm must **immediately, and effectively**, screen that lawyer from any contact with any relevant cases such that **there can be no doubts as to the sufficiency of these measures.**”

Similarly, cases point to the need to obtain affirmative acknowledgments from affected parties (Papyrus Technology Corp) and to enumerate precise details of the screen, including defined sanctions for breach: **Burgess-Lester v. Ford Motor Co.** [2008 U.S. Dist. Lexis 83268 (N.D. W. Va.)].

In non-screening situations organizations mandating confidentiality often stipulate specific requirements. For example, clients may outline parameters as part of outside counsel guidelines, or ask firms to attest to their capabilities in RFP responses. Similarly, several government agencies, either domestically or internationally, have defined specific confidentiality requirements that apply to law firms. For example, in the United Kingdom the Financial Services Authority mandates that individuals with the capability to access insider information be identified and tracked, regardless of whether they have actually accessed said information.

With such a broad variety of confidentiality rules and requirements, the safest bet for firms is to build and maintain the capability to satisfy the most stringent standards.

Updating Firm Confidentiality Protections and Processes

Firms have several options available to examine and address confidentiality practices within their organizations. In most instances, the best place to start is with a review of the current state of firm policies, practices and standards. Conducting a simple internal assessment can help the firm understand the specific confidentiality drivers it commonly faces, how confidentiality is presently managed and, most importantly, how to identify any gaps between policy and practice.

While organizations may choose to conduct an internal survey themselves, engaging an outside expert is often the best strategy. One advantage an outside entity brings is perspective gained from working with other firms and expertise in confidentiality trends and industry standards. Similarly, a third party provides a forum for internal parties to speak more openly about any concerns they have or deficiencies they’ve observed. Finally, this approach is often the most cost and resource efficient. (It’s a little known fact that many insurance underwriters will actually cover the cost of such services. Speak with your firm’s broker to see if your firm can take advantage of funding available for this type of risk consulting.)

As assessment exercise should identify relevant stakeholders and explore a series of topics tailored to the responsibilities and visibility of each respondent. Participants should include risk management, risk operations, IT, and, ideally, a sampling of attorneys and staff. To conduct a thorough analysis, the process should review topics including:

- Existing firm confidentiality policies
- Typical scenarios driving confidentiality enforcement (specific screening scenarios, clients, regulations, etc.)
- Training and education practices
- Notification processes for new confidential matters

- Policy acknowledgment and tracking procedures for specific matters
- Extent and degree to which internal controls are used to enforce access restrictions
- Extent to which firm periodically reviews state of specific confidential matters and screens
- Role technology plays in risk management
- Lifecycle management processes (maintaining notification, acknowledgment, enforcement, and reporting throughout the life of confidential matters)

The result of this exercise should be a report that highlights strengths, weaknesses and areas for improvement based on the specific environment at the firm. Using that information, the organization can respond appropriately, be that through improved training, updated notification procedures or the expanded use of confidentiality enforcement or reporting technology.

Firm Case Study: Automating Confidentiality for Ethical Screens and Confidential Matters

At Kirkland & Ellis, we had an existing confidentiality program in place that we sought to extend in response to emerging trends and business drivers. One set of drivers were the new confidentiality regulations affecting our office in the United Kingdom. Additionally, as a large international firm, we add multiple lateral attorneys each year. While we already had the means to implement screens when necessary, we wanted to streamline, enhance and reduce the resources required to manage those existing processes. Finally, our firm continually invests in staying at the forefront of loss prevention and risk management.

Looking at trends in case law, rules of professional responsibility and client interest, we felt that adopting new technology would best help us continue to enhance our existing confidentiality practices. So we undertook a strategic initiative to investigate and evaluate available choices. As part of our due diligence process, we reviewed several options and selected a product from the leading vendor specializing in these risk and compliance issues. This vendor's technology had been successfully adopted by many of our legal industry peers as the acknowledged standard for confidentiality management.

Provided as a web-based application, the tool we selected enables our firm to centrally control, monitor and report on user access permissions across multiple software applications. It also automates notifications to individuals subject to specific policies and tracks acknowledgments for compliance purposes. The specific areas this technology helps our firm address include:

- Screening Memo Creation
- Attorney and Staff Notification
- Policy Acknowledgment Tracking
- Access Control Enforcement
- Access Control Updates (In response to attorney activity such as time entry records or changing matter team assignments)
- Notification
- Management Reporting

The Selection and Evaluation Process

Because our firm is a large organization with a complex IT environment, it was important that the chosen technology work well with our existing tools, processes and policies. Moreover, in order to minimize disruption and unforeseen surprises, we wanted to make sure that the vendor delivering this solution had an established and proven record for client success – the quality implementation services and ongoing support we would receive was very important to our IT and risk teams. To verify vendor claims to our satisfaction, we conducted reference checks and interviewed relevant stakeholders at peer firms. In the end, only one vendor was able to meet all of our specific requirements.

Firms building decision criteria for their own confidentiality initiatives may have different underlying compliance drivers,

continued

functional requirements and technology preferences. But our priorities include six common-sense criteria which are presented here as a resource for firms engaging in their own evaluation process:

- **Product Maturity and Quality** – Some organizations may have a high tolerance for risk, but being a risk-adverse organization, we wanted to make sure that the technology we put in place had been tested and proven with a track record at peer firms.
- **Scalability** – Similarly, we wanted to make sure our security enforcement tool was suited to deliver security in real-world environments. In this case, the product we selected had already been deployed by an active roster of law firms who were using it to secure over 150 million documents globally.
- **Integration with Existing Environment** – Core to a confidentiality software application is the enforcement of access restrictions across relevant information repositories. In our specific case, this meant the ability to manage access controls across our document management, records management and portal software applications. We also wanted to make sure that the software could automatically extract client and matter information from relevant firm applications in order to streamline policy creation (e.g. easily identify attorneys who should receive a particular screening memoranda). Finally, we wanted to integrate monitoring of our time entry application, to automate alerts and updates in instances where an attorney bills time to a party on one side of a dual-adverse party ethical screen.
- **Logging, Audit and Reporting Capabilities** – Central to effective compliance is the ability to quickly and accurately verify that policies are in place and being followed. We needed the ability to automatically log and report on the audit trail for each confidential matter or restriction. Most importantly, we wanted the ability for risk operations staff to generate these reports directly, without having to use additional third-party reporting software or draw on IT or technical analysts to undertake one-off projects.
- **Ease of Administrative** – Similarly, it was imperative that our choice of technology reduce burdens on risk staff, IT resources and attorneys. The firm did not want to bring on or assign additional personnel to improve ethical screen and confidentiality management processes, nor did it want to add additional red tape for attorneys requesting or responding to confidentiality policies. Addressing these issues called for a tool that would enable us to automate and streamline processes such as policy notification and acknowledgment tracking. In addition to previously mentioned requirements for policy creation and reporting, we also wanted the ability for risk staff to create and modify access control restrictions without intervention and assistance by IT staff.
- **Vendor Reputation** – Finally, with so much resting on these issues, we wanted to work with a technology provider who could point to past success and future partnership. Our firm had specific process requirements and was able to work closely with the vendor to map their technology to our needs and to incorporate our requirements into future product development. Similarly, we wanted to make sure the vendor was forecasting and responding to industry trends so the capabilities of the product would continue to expand and mature – we did not want to face a situation where law firm practices and standards evolved in ways that we were not prepared or equipped to address. In our case, our partner vendor is actively involved in shaping these trends and by working with them we're able to limit the risk of unexpectedly falling behind.

Conclusion – The Expectations are Rising

Given the increasing attention placed on confidentiality, it's prudent for firms to look seriously and re-evaluate their existing practices. With new rules, new precedents and new information technologies continuing to complicate and inflate the ways in which information is created and communicated, the risk of unexpected incidents, breaches or gaps is increasing. Thankfully, educational resources, technology and services exist which can enable organizations to enhance their capabilities and reduce risk. As more firms adopt more rigorous approaches to managing confidentiality and compliance, they're creating stricter de-facto standards and expectations for the legal industry as a whole. In this context, every firm should carefully consider the state of confidentiality management in their environment, as this is an issue whose profile will only continue to grow.

