

Risky Business

Walking a Fine Line

ILTA White Paper **October 2011**

Ethical Walls and Confidentiality Screens: Not Just for Conflicts

NANCY BEAUCHEMIN **INOUTSOURCE**

Historically, law firms implemented most ethical walls and confidentiality screens in response to an identified potential conflict between existing and former clients in new representations. Evolving legal requirements surrounding client confidentiality and data privacy concerns are among the risks forcing law firms to re-evaluate their technology infrastructure and policies for securing client matter information subject to an ethical wall or confidentiality screen.

NEW CLIENT AND REGULATORY REQUIREMENTS

It is presumed that lawyers understand all of the complexities of their obligations to serve clients in accordance with professional responsibility guidelines and evolving legal statutes. Law firms are under tremendous public scrutiny and pressure. Several high-profile firms have found themselves defending lawsuits that may have been avoided if there had been adequate controls in place for managing client relationships and their confidential information throughout the matter representation.

Screens are often erected to avoid disqualification as a result of an attorney's prior work history with another firm, organization or government. In simplistic terms, the function of a screen is to ensure that confidential information known to a disqualified attorney is protected and not disclosed to others

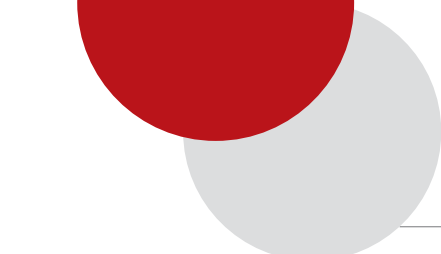
in the firm who are working on the matter. Today, law firms are applying confidentiality screens for a variety of reasons, including an increasingly complicated legal and regulatory environment that demands compliance with record-keeping requirements defined by their clients. Law firms are realizing that they must know where their information resides and how it is accessed and stored before they can protect it from inadvertent disclosure. Clients will sometimes exercise their right to audit a firm's internal record-keeping processes to ensure compliance with their guidelines. In a legal proceeding, courts will require evidence that policies were consistently followed.

According to Chubb & Son's "A Lawyer's Guide to Records Management Issues," "An effective records retention policy should ensure that documents are stored only in identifiable locations, appropriately backed up, and treated consistently wherever they are located and in whatever media they exist."

A firm's IT department is often the last to know when client information requires an ethical or confidentiality screen for reasons other than in response to a potential conflict of interest.

CLIENT INTAKE AND CONFLICTS DUE DILIGENCE

A survey by Ames & Gough of insurers that provide coverage to law firms ("Lawyers' Professional Liability Claims Trends: 2011") revealed that malpractice claims have increased substantially in 2011. In bad economic times, it is not surprising that



unsatisfied law firm clients will seek financial restitution through a lawsuit. Many of the asserted claims are because of conflicts of interest. According to the Ames & Gough survey, “If the lawyers representing a client are not careful during the initial representation, they might well become targets for a malpractice claim as the client’s financial situation worsens.” One of the primary goals of a law firm’s client intake and conflicts due diligence process is to ensure that a lawyer’s duty of loyalty and confidentiality to his or her clients is not breached.

Increasingly, clients provide their outside counsel with their own retention agreement that stipulates provisions for ensuring that their confidential information is protected and restricted to only the legal team assigned to handle the representation. Bank of America’s “Outside Counsel Procedures,” for example, state in part, “Outside counsel is responsible for establishing appropriate ethical walls within the firm to restrict access to any legal matter file to those users with a business reason to access the matter.”

Traditional law firm client intake and conflicts due diligence workflow processes may need to be updated to take into consideration client-mandated procedures surrounding confidential management of information. Firms need to establish protocols to automatically notify the IT department when matters are opened that require confidential information access be limited to the legal team working on the matter. Many law firms’ client intake workflow processes do not have a validation mechanism to ensure that outside counsel’s confidentiality requirements are reviewed and understood by IT. A recommended best practice is to routinely review the firms’ larger clients’ outside counsel guidelines and procedures. Once reviewed, there should be a process to audit compliance with confidentiality requirements.

EMERGING PRIVACY LAWS

Recent updates to Health Insurance Portability and Accountability Act (HIPAA/HITECH) laws, along with state privacy guidelines (such as Massachusetts 201 CMR 17:00 Data Privacy legislation), serve to protect inadvertent disclosure of protected health information and personal identification information. Massachusetts 201 CMR 17:00 defines personal information as “a Massachusetts resident’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number.”

Personal information as previously described could potentially exist in various types of legal representations, including trust and estate, bankruptcy, corporate, banking and securities, personal injury and litigation matters. These laws provide minimum standards that must be met to safeguard

personal information. Massachusetts 201 CMR 17:00 states in part, “Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical and physical safeguards.” If standards are not met, breaches in security can be costly to a firm. Law firm IT managers need to work with the firm’s general counsel and executive management to understand that specific client representations might contain personal information and to know where this information resides within firm systems and applications. Once this information is identified, it must be secured.

ITAR CONSIDERATIONS

International Traffic in Arms Regulations (ITAR) specifies a list of articles, services and technology in the United States Munitions List (USML) that could be designated as defense related. While it is assumed that most materials on the USML are manufactured by defense contractors, there are other items such as cameras and facsimile equipment that are also on the USML. If your firm has an intellectual property (IP) practice, it is conceivable that those matters contain information that is subject to ITAR regulations. One of the provisions of ITAR is that only United States citizens, as defined in section 120, paragraph 15, are allowed to access restricted information. Firms should take care to know the ITAR requirements and establish screens to avoid disclosure to non-U.S. citizens, including employees of internal and external support staff.

CONFLICTS OF BEING A MEMBER OF A BOARD

Although many bar associations caution lawyers against performing board service for clients, many lawyers serve on boards of both public and private entities. If the entity for which a lawyer is serving is a client of the firm or becomes a client, there is the possibility for conflicts because the lawyer has a duty to the firm as well as an obligation to the board on which he or she serves. ABA Formal Opinion 98-410: “Lawyer Serving as Director of Client Corporation” was issued to address some of the complex issues that arise when attorneys serve on boards of their clients.

For example, let’s assume that a lawyer at your firm is serving on the board of a local private university. The university is contemplating constructing a dormitory. However, the designated site for the proposed dormitory will require a zoning variance and an access road to be built. Your firm has expertise in working with municipalities and has had success with obtaining zoning variances on behalf of other clients. If the university hires your firm to handle the zoning issues, the lawyer

who serves on the board will benefit. Entities where lawyers are performing board service should disclose their service to the firm and this information should be noted in the firm's conflicts database. Just as it is the responsibility of lawyers to notify their client intake and conflicts system of new parties that may be identified in a matter, it should be a firm policy that lawyers disclose board service opportunities to the firm. In law firms where board service is allowed, there should be mechanisms in place to ensure that the lawyer's board member service does not conflict with existing duties to current and former clients.

In many situations, conflicts that arise as a result of lawyers serving on boards of clients can be waived by the client. Usually as a condition to consent to waiver of conflict, it is expected that the lawyer/board member will be screened from accessing client matter information for entities that are represented by the firm.

DON'T FORGET ABOUT SUPPORT SERVICES

Scanning hard copy documents has increased in firms as many legal teams prefer to manage matter information electronically. While some lawyers and secretaries do their own scanning, it is commonplace to delegate scanning tasks to either an internal or external office services department.

Internal office services personnel will often scan hard copies and save those images to an open network drive. Depending upon the workflow and security measures established, these imaged documents may contain personal or confidential information that should be protected and made inaccessible to inappropriate parties within the firm.

As stated earlier, there are several emerging privacy regulations to consider in these scenarios. Massachusetts 201 CMR 17:00 stipulates that email messages that contain personal information should be encrypted. HIPAA/HITECH also has provisions for protecting disclosure of personal health information (PHI). Both of these laws have breach notification requirements to which law firms must adhere. Law firms need to be aware of these strict requirements and exercise control over support service providers that have access to personal information.

ROADMAP TO SUCCESS

IT leaders should take an active role in preparing their law firms to address the need for ethical walls and confidentiality screens. The following steps will help identify the deficiencies in your firm's policies and practices.

- **Identify Confidential Information:** The first step is to identify where confidential client matter information resides. Create a data map for all firm applications and repositories. If confidential client information resides in repositories that cannot be controlled through a confidentiality screen, there

should be a plan to migrate this confidential information to repositories that can be secured.

- **Restrict Access:** Once you have identified confidential information that needs to be protected, your firm should have established, tested processes for restricting access to this information. Technology solutions can automate this process.
- **Provide Mandatory Education:** Law firms need to have ongoing education for attorneys and staff to make them aware of emerging data privacy regulations, and sessions should be mandatory. Attorneys should acknowledge their understanding of confidentiality, especially as it applies to matters with which they are directly involved. If your law firm has locations across multiple jurisdictions, someone must be responsible for knowing the data privacy laws in those areas. With some regulations, it is required to notify authorities of data breaches, especially if the breached data contained personal information.

MAKE SURE PROPER SCREENS ARE IN PLACE

Ideally, repositories and applications that store confidential client matter information should be centrally maintained and managed by a firm's IT department, and all client matter information should be readily identifiable by the applicable client matter.

The screening function should be centralized within the office that is primarily concerned with risk management and loss prevention issues. This is sometimes the responsibility of the firm's general counsel. There must be immediate and direct communication with affected users, records and IT staff. Screening processes should be documented and require affected individuals to acknowledge and comply with the screen. Screens should be regularly reviewed and removed when no longer needed. There should also be policies to notify appropriate governing bodies and clients of data breaches.

Law firm confidentiality policies are often disconnected from requirements mandated by clients and regulatory bodies. Firms need to understand where they have gaps and commit to correcting deficiencies in policies and use of technology to ensure that their clients' confidential information is protected. **ILTA**

NANCY BEAUCHEMIN is the President of InOutsource. She has spent more than 20 years advising law firms on records and information management best practices given rising costs, new technologies and evolving risk management concerns. Nancy has earned the Certified Records Manager (CRM) designation, she frequently speaks to audiences on the challenges of managing information, and she has authored several articles for legal and information management publications. Nancy can be reached at nbeauchemin@inoutsource.com.