CLM CLAIMS & LITIGATION MANAGEMENT ALLIANCE™

ADVANCING ETHICS, COOPERATION AND EDUCATION

2016 CLM Boston Conference
July 14-15, 2016
Boston, MA

Lawyers: Global Perspectives on Data Collection, Transfer, Use and Disclosure

Financial exposure to law firms and their clients is an inherent risk in data collection, transfer, use and disclosure, and the proliferation of computers, mobile devices and information systems has profoundly increased that risk. The quick pace and flow of information in a highly mobile environment have created dangerous pitfalls for law firms and their clients. At the same time, law firms are historically less vigilant with regard to internal controls and cyber defense in contrast to other industries.

These historically weak controls have resulted in a series of cyber-attacks from all over the globe recently. For example, cybersecurity firm Flashpoint issued an advisory alert in February reporting that nearly 50 prestigious law firms were targeted by foreign hackers looking for insider information. Not only do criminal enterprises see law firms as a gateway to access insider information, but "hacktivists" may see corporate lawyers as the soft underbelly of the financial sector. Often overlooked are the risks from dishonest, disgruntled, or untrained employees or independent contractors.

I. LEGAL ISSUES

In response, the legal profession has become the focus of a wave of new legal, regulatory and ethical rules. An attorney is well advised to consult the professional responsibility rules, comments, and ethics opinions in the relevant jurisdiction(s). For instance, most states now require attorneys using technology to take competent and reasonable measures to safeguard client data. This duty extends to all use of technology, including without limitation computers, mobile devices, networks, technology outsourcing, and cloud computing.

The rise in data breaches and threats has been accompanied by a rise in regulator activity, both at the state and federal level. Regulators do not discriminate based on the type or sophistication of data compromise. Whether a data compromise takes the form of a lost laptop, lost iPhone, improperly emailed documents, improperly disposed documents, phishing attack, or sophisticated network hack, regulatory obligations and the risk of regulator scrutiny exist.

Law firms need to be aware of a network of overlapping state and federal laws. These laws impose obligations on law firms and the firms' clients regarding the storage, security, use, and transmission of data, and may require that firms provide written notice to individuals, regulators, and the media in the event of a breach of protected data.

Many federal and state laws impose affirmative obligations on entities, including law firms, to protect certain data in their possession, whether originating from clients or not. Most notably, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), impose obligations on entities that, among other things, use, store, create, and transmit protected health information ("PHI"). Firms that represent health care entities need to be aware of these obligations. Not only does a firm need to understand the risk HIPAA imposes on its clients, but, as a potential business associate to a HIPAA covered entity, firms need to be aware that they are directly regulated by HIPAA. The 2013 HIPAA-HITECH Omnibus Final Rule made clear that the Department of Health and Human Services has the ability to regulate, and fine, not only covered entities, but also business associates, which may encompass a law firm handling protected health information on behalf of its clients. 78 FR 5566. As a result, law firms need to ensure that they protect client data for the sake of both their clients and themselves.

Attorneys also need to be aware of the various state data protection and notification statutes, both those that include affirmative obligations and the 47 separate state laws (not including territories like Puerto Rico and the U.S. Virgin Islands) that mandate notice in the event of unauthorized access or acquisition to protected information. In every state, protected information includes a Social Security number, driver's license number, and financial information. Many states broaden the definition to include dates of birth, medical information, user names and passwords. State and federal regulators often impose fines on entities that suffer a breach of protected information. For instance, in March 2016, a health care entity was fined $1.55 million when a business associate lost a laptop containing information related to 9,000 patient records. The primary reason cited for the fine was the lack of a business associate agreement in place. Thus, not only can firms expose themselves to financial and reputational harm, but the failure to properly document a business associate relationship may also subject their clients to substantial harm.

Internationally, the problem becomes even more complex, as organizations with multinational operations that transfer data between countries are often subject to varying requirements between nations, including those of the individual EU countries. The laws are continuing to evolve in the wake of greater concerns among these countries about US data breaches and access by US surveillance agencies, and have become extremely stringent in terms of coverage and consequences. While the focus of these laws is generally on "processing" of personal information, the definition may be very broad and include any operation or set of operations performed on such data, such as collection, recording, transfer, disclosure, disposal, storage, use, backing up and even organization. Consequences may include damage claims, large

administrative fines for individuals and organizations, criminal actions, and imprisonment. The situation has become increasingly urgent in the wake of the October 2015 decision by the European Court of Justice in *Maximillian Schrems v. Data Protection Commissioner* (Case C-362/14). In that case, the Court determined that the Safe Harbour Principles established by the U.S. Department of Commerce in consultation with the European Commission, upon which thousands of entities had been relying for years for cross-border transfers of such data, provided insufficient guarantees, and declared as "invalid" the European Commission's Decision 2000/520/EC of 26 July 2000 on the adequacy of such principles.

II. ETHICAL DUTIES

In addition to legal and regulatory burdens facing law firms, it is critical to understand the ethical obligations that apply. For law firms with a large geographic footprint, a patchwork of states rules may apply.

A. Competence (ABA Model Rule 1.1)

1. General Rule: A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

2. Competence includes selecting and using technology. It requires attorneys who lack the necessary technical competence for security to consult with qualified people who have the requisite expertise. In other words, the duty of competence requires attorneys to know what technology is necessary and how to use it.

B. Communication(ABA Model Rule 1.4)

1. General Rule: A lawyer shall: (1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules; (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished; (3) keep the client reasonably informed about the status of the matter; (4) promptly comply with reasonable requests for information; and (5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

2. A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

3. Requires notice to a client of compromise of confidential information relating to the client.

C. Confidentiality (ABA Model Rule 1.6)

1. General Rule: A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation. A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

2. This rule it is not limited to confidential communications and privileged information. Generally, an attorney must obtain a client's express or implied consent (in the absence of special circumstances like certain misconduct by the client).

3. The rule prohibits an attorney from disclosing "information relating to the representation of a client" unless the client consents to the disclosure or one of the exceptions to the confidentiality rule applies. The rule is broader than the attorney-client privilege evidentiary rule. Confidentiality survives and obligates a departing attorney and the former firm.

4. Comment 16 to Rule 1.6 requires reasonable precautions to safeguard and preserve confidential information: A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

III. Common Law Duties

Along with the ethical duties, there are common law duties to protect data belonging to clients and third parties. Breach of these duties can result in a malpractice action, a claim that failure to protect privileged information was a breach of the attorney's fiduciary duty, or inadvertently waived the attorney-client privilege.

IV. Contractual Duties

Under pressure from clients to bolster data security, law firms may agree to implement enhanced security measures to keep the revenues flowing. Acceptance of contractual duties to protect client (or client's client) data (especially health care and financial information), without a commitment from firm leadership to take it seriously, could expose the firm to significant losses, however.

V. Risk Management

In addition to taking an assessment of the risks unique to your law firm, consider implementing the following measures:

- An essential part of preparedness is testing out the incident response plan and making sure it's right for the firm. At a minimum, the incident response team should include all the senior managers in any department that might be implicated in a breach, as well as the compliance head, chief information officer, chief information security officer, IT department, human resources head and the marketing director.

- As part of the incident response plan, employee training programs and initiatives around cyber and information security, compliance procedures and ethics must be conducted on a regular basis. Consider what security measures are right for your law firm.

- From the moment a breach is revealed, an incident response team needs to be able to get into formation and respond to a crisis that will yield new demands and challenges by the minute. If the team members have practiced and refined their response, they're much more likely to minimize damage to the law firm, its systems and its clients whose information might have been stolen or compromised.

- Screen vendors and other third parties with regard to security measures. When onboarding or reviewing these vital business relationships, a firm should also require acknowledgement it will comply with the firm's code of conduct and contractually require their compliance with the firm's data protection policy and all applicable laws. Monitoring, controls and remedies should also be evaluated.

- Invest in encryption technology. Encryption is an effective risk management tool, especially considering the prevalence of data breaches, and resulting fines, stemming from lost or stolen laptops. Many statutes include a safe harbor for lost data if that data is encrypted, so encrypting laptops and tablets is simple solution to this problem.

- Implement two-factor authentication. Security experts praise two-factor authentication as one of the most effective risk mitigation tools available. Numerous high profile breaches originated after the theft of high-access credentials, whether by phishing, malware, or social engineering. Two-factor authentication substantially reduces the risk of credential theft.

- Ensure compliance with BYOD polices. Remote access via phone, tablet, or laptop are essential to an attorney's practice. Ensure that the firm has and implements a BYOD policy that tracks unique devices and ensures adequate technology, like encryption and

two-factor authentication, software patching and virus protection are implemented on remote devices, whether supplied by the firm or individually purchased. Remote tracking and wiping applications are also available and should be considered.

- Law firms should think seriously about cyber insurance as part of an overall enterprise risk management framework. Cyber insurance can strengthen a firm's data security practice by fostering a dialogue between practice managers, clients, vendors and brokers of cyber risks. Cyber insurance also serves as a catalyst to forge relationships with outside breach coaches and security specialists.