ASPEN PUBLISHERS

The COMPUTER & INTERNET Lawyer

Volume 28 ▲ Number 10 ▲ OCTOBER 2011

Ronald L. Johnston, Arnold & Porter, LLP Editor-in-Chief*

Lawyers and Data Security: Understanding a Lawyer's Ethical and Legal Obligations That Arise from Handling Personal Information Provided By Clients

By Matthew H. Meade

In the midst of a heated labor law class action, Law Firm A produces to Law Firm B an encrypted CD containing an Excel spreadsheet identifying a group of its client's employees by name, birth date, hire date, and Social Security number. An intrepid associate at Law Firm B downloads the spreadsheet to his laptop in unencrypted format so that he can review the data during his flight to a deposition on the West Coast. The laptop and the data on the laptop are then stolen from a security checkpoint at the airport. The associate promptly reports the theft to the airport police and to the IT department at Law Firm B. As a result of the stolen laptop, Law Firm A, Law Firm A's client, and Law Firm B are in the midst of a data breach involving the personal information of employees of Law Firm A's client. Law Firm A and Law Firm B need to immediately begin evaluating their respective obligations to provide notice of the breach under applicable state law and their ethical obligations with respect to the missing data.

This article will explore the panoply of issues that arise when lawyers are involved in data security incidents similar to the Law Firm B example by focusing on the following four areas:

1. Recent news headlines regarding data breaches arising from the actions or inaction of attorneys;

2. The root causes of those incidents;

3. The current ethical and legal framework applicable to lawyers who are involved in data breach incidents; and

Matthew H. Meade is a shareholder in the litigation practice group and the Co-Chair of the Data Security and Privacy Group in the Pittsburgh office of Buchanan Ingersoll & Rooney PC.

Wolters Kluwer
Law & Business

4. Suggested best practices to help attorneys develop stronger data security practices.

The Headlines

Over the past several years there has been a small number of reported data breaches involving lawyers. It is not clear why data breaches in the legal profession are not more widely reported, but it may have something to do with the nature of the attorney-client relationship and the desire to keep the breaches out of the public eye. The impact on a law firm that gains a reputation as being unable to protect confidential data, particularly client data, could be devastating to its image, its ability to retain and attract clients, and its standing in the legal community.

As set forth in more detail in this article, the reported data breaches involving lawyers fall into three main categories: (1) careless disposal of client records; (2) theft of mobile devices; and (3) misuse of internal security protocols.

Document Disposal Issues

Most of the reported incidents of attorney data breaches involved small law practices that discarded paper records with client personal information without shredding or otherwise rendering the records unreadable. For example, in October 2010, a California lawyer mishandled the records of eight prison inmate clients who had been found guilty of murder.[1] The attorney discarded records that contained the names, criminal histories, psychological evaluations, Social Security numbers, and observations about family relationships and behavior in prison of the inmates in a public dumpster.[2]

In July 2010, an Illinois bankruptcy attorney discarded hundreds of personal and financial documents of his clients, including client authorization sheets with Social Security numbers, names, addresses, driver's license numbers, and signed debit card authorizations.[3] The attorney explained that the documents in bags marked "do not remove" had been transferred from one office to another in order to be shredded. He suspected that cleaning employees removed the bags, despite the warning sign on the bags.

Later in July 2010, a San Antonio lawyer left legal files of former clients in a public dumpster.[4] The documents contained names, addresses, bank account information, Social Security numbers, driver's license numbers, and dates of birth.[5] The attorney acknowledged disposing of the files and added that he was unaware of any state law governing the secure disposal of client records.

In October 2010, an Indiana lawyer left boxes of client records unsealed next to dumpsters already overflowing with trash.[6] The contents of the lawyer's boxes "went flying into public view" because the boxes were not properly secured.[7]

Stolen Equipment

Like other industries, stolen equipment is one of the leading causes of data breaches in the legal field. For example, in June 2006, a lawyer working for the Social Security Administration violated a work-at-home agreement and brought a laptop with sensitive information to a conference in Atlanta where it was stolen.[8] Social Security numbers, names, and possibly medical information were stored on the stolen laptop.

In April 2008, a thief stole a laptop from the car of a Baltimore sole practitioner that contained unencrypted information related to tax returns of 100 clients.[9] The attorney also stored personal data on the laptop related to any dependents whose names may have appeared on the tax returns.

Verizon's 2010 Data Breach Investigation Report concluded that privilege misuse is the primary reason that data breaches occur.

In December 2008, a password-protected, unencrypted disk with names, Social Security numbers, and other personal information was stolen, together with computer equipment, from a secure safe at an offsite storage facility.[10] The data identified lawyers who performed work for the Central California Appellate Program, which supplies lawyers for indigent appeals.

In July 2010, a thief stole a laptop from the home of a New Hampshire family law practitioner.[11] The laptop, while password protected, was not protected by any encryption software. The attorney stored names, Social Security numbers, tax identification numbers, and account numbers on the laptop. The attorney immediately notified the police of the break-in.

In September 2010, the court-appointed claims agent for the liquidation of Madoff Investment Securities reported the theft of a password-protected laptop from a locked employee's car.[12] The laptop had personal information including Social Security numbers, names, and addresses of individuals who had accounts with Madoff Investment Securities.

Internal Security Protocols Bypassed

The following examples of lawyer data breaches arise in the context of the production of or access to

confidential data. Despite having procedures in place to prevent unauthorized access, the internal protection systems were bypassed either through human error or duplicitous conduct.

In January 2010, Morgan Keegan & Company of Memphis produced to the Alabama Securities Commission client documents related to an ongoing multistate securities investigation. The documents contained Social Security numbers, ages, incomes, net worth, and other account information of Morgan Keegan clients.[13] Morgan Keegan had received assurances prior to production that the data would be treated as confidential by the Alabama Securities Commission. In April 2010, the Alabama Securities Commission issued a show cause order to revoke the registration of Morgan Keegan. The Securities Commission downloaded the order to a secure network with redacted versions of the exhibits attached. An unredacted and redacted disk with the exhibits was delivered to the Alabama Securities Commission's file room.[14] A plaintiff's law firm could not access the Morgan Keegan data from the secure Web site and contacted the Securities Commission to get a copy of the order and the exhibits. The Commission inadvertently produced an unredacted copy of the exhibits to the lawyer for some of the investors who claim to have been harmed by Morgan Keegan.

Morgan Keegan discovered the breach in September 2010 and provided notice later in September to its impacted customers. In addition, the Alabama Securities Commission conducted a detailed investigation of the incident and concluded that "the inadvertent copy of the disk was the result of the use of new technology (hyperlinks) in an administrative order for which long standing procedures failed to address all possible security concerns."[15]

In May 2010, in response to a Freedom of Information Act request, a Virginia school district produced personally identifiable information of school employees, including Social Security numbers.[16] The PDF attachment identifying the employees was included with approximately 350 other email attachments.

In late December 2010, Experian provided notice that someone at a California law firm had used the firm's Experian log-in credentials to access multiple credit reports that included Social Security numbers, dates of birth, and other account information without proper authorization.[17]

Root Causes of Law Firm Data Breaches

Verizon's 2010 Data Breach Investigation Report, prepared with assistance from the Secret Service, concluded that privilege misuse is the primary reason that data breaches occur, followed by hacking, malware, social tactics (*e.g.*, phishing, spoofing, scamming), and physical attacks, such as stolen laptops.[18]

Misuse is defined in the Verizon report as "using organizational resources or privileges for any purpose or in a manner contrary to which it was intended."[19] Examples of misuse given in the Verizon report include abuse of system/access privileges, handling of data in an unapproved format, abuse of private knowledge, storage/transfer of unapproved content, and violation of asset/data disposal policy.[20]

The examples of careless document disposal by lawyers, inadvertent production, and improper use of authorized credentials fit squarely within the Verizon definition of misuse and, consistent with the findings in the Verizon report, clearly emerge as the single leading cause of attorney data breaches. Surprisingly, none of the reported lawyer data breaches involve hacking, malware, or social attacks. Physical attacks like theft, however, are the next leading cause of data breaches for lawyers.

Ethical and Legal Standards Applicable to Lawyers Handling Client Data

Armed with a basic understanding of the kinds of breaches lawyers are experiencing and the causes of those breaches, it is important to analyze the ethical and legal consequences of those incidents. Rather than talk in abstracts, throughout this section the article will use the Law Firm B incident highlighted in the introduction and the Indiana lawyer who discarded boxes of client files to understand the ramifications of attorney-caused data breaches.

State Ethics: Rule 1.6 Confidentiality of Information

All 50 states have an ethical rule that provides that a lawyer shall not "reveal information related to the representation of a client unless the client gives informed consent," subject to certain exceptions including preventing a criminal act and preventing the client from committing a fraud. (*See* Rule 1.6). Twenty-nine states[21] and the District of Columbia have comments to Rule 1.6, which specifically address a lawyer's obligation to act competently to preserve confidentiality. The comment states that:

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of

> communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

The comment requires "reasonable precautions" to prevent unauthorized access to client communications and not "special security measures." As written, the comment can be construed to mean that lawyers need not encrypt client emails or client data as a matter of course. The comment goes on to clarify the attorney's obligation, however, and notes that certain situations may warrant "special precautions," including the sensitivity of the information and the extent to which the information is protected by law. Under this "special circumstances" analysis, a lawyer email that attaches a spread sheet with Social Security numbers of a client's Massachusetts employees would need to be encrypted to comply with Massachusetts law requiring encryption of personal data.

There is, however, no discussion in the comment regarding a lawyer's obligation with respect to the confidential information supplied by an adversary (the Law Firm B incident). Would it be considered a violation of Rule 1.6 if Law Firm A, knowing the nature of the data that it produced to Law Firm B, failed to take any precautions to ensure that Law Firm B would continue to maintain the data in encrypted format? The analysis would hinge on the reasonableness of failing to take steps to protect the data once it went to a third party.

Violations of this standard can lead to attorney sanctions. For example, on September 30, 2010, the Indiana Supreme Court issued an opinion calling for a public reprimand of an attorney for, among other things, a violation of Rule 1.6(a).[22] The attorney asked his adult children to dispose of 12 to 14 boxes of client files. The children took the boxes to a recycling bin and left them on the ground next to the full bins. The tops blew off the boxes and scattered the files into public view. As soon as he learned of the incident, the attorney retrieved the boxes. There is no indication that personal information of the clients was included with the exposed files.

Two recent ethics opinions have specifically addressed Rule 1.6 and the obligation to act competently in connection with client data. On December 13, 2010, the Florida Bar Ethics Committee issued Opinion 10-2 and concluded that lawyers who use devices that contain "Storage Media such as printers, copiers, scanners and fax machines" have an affirmative obligation to take reasonable steps to ensure that "client confidentiality is maintained and the device is sanitized before disposition."[23] A lawyer who chooses to use any of these devices has a duty of competence from the moment of receipt of the particular device, through the life cycle of the device, and once the device is disposed. The reasonable steps that a lawyer must take to ensure confidentiality include: (1) identification of potential threats and development of policies to address the threats; (2) inventorying all devices that contain hard drives that store media; (3) supervising non-lawyers; and (4) "sanitization of any device by requiring meaningful assurances from vendor confirming sanitization."[24] Interestingly, in connection with identifying potential threats the opinion includes a requirement that the lawyer "keep abreast of changes in technology to the extent that the lawyer can identify potential threats to maintaining confidentiality."[25] Keeping abreast of technology is an onerous burden, particularly in the area of data security because of the constantly evolving playing field. Florida has now established a precedent under which a lawyer who fails to keep current with data security protection could be found to have violated his or her ethical obligations to the client.

In 2010, the Standing Committee on Professional Responsibility and Conduct in California issued an opinion addressing whether an associate who uses his firm-issued laptop outside of the office would violate his duty of confidentiality.[26] The committee concluded the use of the laptop was not problematic because "access is limited to authorized individuals to perform required tasks."[27] The committee was troubled by the use of the laptop on a public wireless connection, concluding that such use "risks violating [the lawyer's] duty of confidentiality and competence . . . unless he takes proper precautions such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall."[28] The committee added a warning that because of the considerable risk associated with use of wireless networks, the attorney may need to seek the client's informed consent to use the connection.

State Document Disposal Laws

Currently 25 states have laws governing the disposal of records with personal information. The laws

generally set forth an affirmative duty to securely destroy sensitive information that includes personal identifiers, personal information, and, in California,[29] any identifying information. By way of example, Connecticut requires that any party holding personal information of Connecticut residents "shall destroy, erase or make unreadable such data, computer files and documents prior to disposal."[30] Massachusetts law dictates that paper documents containing personal information "shall either be redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed,"[31] and electronic media shall be destroyed so that "personal information cannot be read or reconstructed."[32]

Currently 25 states have laws governing the disposal of records with personal information.

Using the Indiana attorney as an example, in addition to a violation of § 1.6 of the Indiana Code of Ethics, to the extent that there was any personal information of Indiana residents included in the boxes of information, then the attorney would be liable for a Class C infraction under Indiana's document disposal law for "disposing of unencrypted, unredacted personal information of a customer without shredding, incinerating, mutilating, erasing or otherwise rendering the information illegible or unusable"[33] prior to destruction.

Massachusetts Data Security Law

Under the recently enacted Massachusetts law regarding the protection of personal information of residents, "every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information" shall have a written, comprehensive information security program "covering its computers, including any wireless system."[34] Accordingly, a law firm that maintains data regarding Massachusetts residents must have a written information security program.

Using the example of the Indiana lawyer again, his disposal of the client records would be problematic under the Massachusetts data security law,[35] which applies to both paper and electronic records. Assuming that the Indiana lawyer's client records contained personal information of Massachusetts residents, the attorney would be in violation of the Massachusetts law for failing to have "[r]easonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers."[36]

At least nine other states—Arkansas, California, Connecticut, Maryland, Nevada, Rhode Island, Oregon, Texas, and Utah[37]—mandate minimum security requirements for businesses that store personal information. If a law firm processes, collects, or maintains personal information related to residents of these states, it would be obligated to adopt comprehensive data security and privacy programs to protect the personal information.

Encryption under Nevada and Massachusetts Law

Both Massachusetts and Nevada require differing levels of encryption of personal information of residents. Massachusetts requires:

> Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly . . . .
>
> Encryption of all personal information stored on laptops or other portable devices.[38]

Nevada law provides that:

> A data collector doing business in this State who "accepts a payment card in connection with a sale of goods or services . . . shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard . . . ."[39]

The Nevada law also provides that a data collector who does not accept payment cards shall not:

> (a) Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission; or
>
> (b) Move any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information.[40]

Using the breach example involving Law Firm B from the introduction of this article, if the data on the laptop included personal information regarding residents of Massachusetts and Nevada residents, it is clear

that there would be a breach of the Massachusetts law requiring encryption of data on laptops and the Nevada law for moving the data beyond the controls of the collector and not ensuring encryption.

State Data Breach Laws

Six states require notice of a breach involving paper records.[41] If the Indiana lawyer did not retrieve the discarded client records from the dumpster and those records contained personal information, he would be obligated to provide notice if the lost records contained information of residents from any of those six states. As for the remaining 44 states, the California Office of Privacy Protection recommends that, even though California's data breach law applies only to computerized data, the notice standard should be applied to all "records in any media, including paper records."[42] Accordingly, it is considered a best practice to provide notice to individuals of a breach regardless of the form of the record that has been lost or subject to unauthorized access. The Indiana lawyer should provide notice to residents of the other 44 states to the extent that any of their personal information was included in the files left at the dumpster.

Using the Law Firm B example again, a breach caused or arising from a law firm that receives confidential information triggers an obligation under most state laws to provide immediate notice to the data holder. (In this case it would be the producing law firm as opposed to the producing client, given that the ethical obligation not to directly contact a party that one knows to be represented.) The Law Firm B example would require that notice be sent to all individuals whose names were listed on the spreadsheet stored on the lost laptop. In all likelihood, the notice would be best from Law Firm A's client, but the costs associated with responding to the breach, including preparing the notice and offering credit monitoring, should be Law Firm B's responsibility.

Social Security Number Policies

Connecticut, Michigan, New Mexico, New York, and Texas require businesses that maintain the Social Security numbers of residents of their respective states to ensure the protection of the data through the development of internal policies and procedures. In Connecticut, "[a]ny person who collects Social Security numbers in the course of business shall create a privacy protection policy which shall be published or publicly displayed."[43] A business in Michigan that collects more than one Social Security number must create a policy that "ensures to the extent practicable the confidentiality of the social security numbers."[44] New Mexico and New York require the development of a policy or internal regulations to protect Social Security numbers and for maintaining the confidentiality of Social Security numbers.[45] Texas law provides that businesses that require an individual to disclose his or her Social Security number to receive goods or services or enter into a business transaction must have a privacy policy that details how the information is collected, used, and protected; who has access to the data; and how it is disposed.[46] A law firm that has access to employee or client Social Security numbers would be required to comply with these laws and enact specific policies to protect Social Security numbers.

Federal Rule of Civil Procedure 5.2(a)

Federal Rule of Civil Procedure 5.2(a) provides that:

> Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual's social security number, tax payer identification number, or birth date, the name of an individual known to be a minor, or a financial account number, a party or nonparty making the filing may include only:
>
> (1) the last four digits of the social security number and the taxpayer identification number;
>
> (2) the year of the individual's birth.

Two recent decisions highlight a lawyer's responsibilities under this rule and make clear that courts will not hesitate to sanction attorneys who ignore their obligations with respect to confidential personal information in court filings. In *Engeseth v. County of Isanti*,[47] a federal district court sanctioned an attorney for "lack of judgment" when he electronically filed a sworn accounting affidavit with the Social Security numbers of 179 individuals in violation of Rule 5.2(a). The order provided that the attorney was required to notify each individual, provide each individual with credit reports and 12 months of credit monitoring, and make a charitable donation so that the attorney "will keep in mind the interests and safety of dependent parties before he acts in the future."

In *Allstate Insurance v. Linea Latina De Accidentes, Inc.*,[48] plaintiffs' counsel filed a complaint with 160 pages of exhibits that contained the names of minors, their birth dates, financial account numbers, and one Social Security number. Several days after the

complaint had been filed, the defendants moved to dismiss or strike the complaint and have it sealed for violations of Rule 5.2(a). A few months after receiving notice of the improper disclosures in the complaint, plaintiffs' counsel still had not corrected the breach despite a misguided effort to do so using a redaction program. Following *Engeseth*, and noting the lawyers' lack of a sense of urgency, the court sanctioned plaintiffs' counsel and required counsel to notify the individuals of the breach and offer a year of credit monitoring. The court also issued this scathing rebuke in its opinion:

> the days of attorneys being able to ignore the computer and shift blame to support staff in the event of an error are gone. The consequences are simply too serious. To the extent there are attorneys practicing in federal court who are under the impression that someone in the Clerk's office will comb their filings for errors and call them with a heads-up, the Court delivers this message: It is the responsibility of counsel to ensure that personal identifiers are properly redacted.[49]

HITECH HIPAA Business Associates

A law firm that performs legal services for an entity covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), such as a hospital, that involves the use of identifiable health information can be considered a business associate (BA) under HIPAA. A BA is defined as an entity that, on behalf of a covered entity, performs or assists in performing activities that involve the disclosure of individually identifiable health information (including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing) or provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity.[50]

Under the HITECH Act, all HIPAA Security Regulations relating to administrative, physical and technical safeguards, as well as certain documentation requirements for electronic-protected health information (EPHI) that currently apply to covered entities will apply to BAs.[51]

As a result, law firms that handle EPHI for covered entities will need to adopt administrative safeguards such as developing policies and procedures, appointing a security officer, establishing sanctions for violations, providing regular training and perform regular evaluations of policy effectiveness.

In connection with physical safeguards, BAs must implement safeguards for workstation security; develop policies for disposition of EPHI on workstations; and develop policies for hardware removal.

The technical safeguards required for BAs include assigning unique names or numbers for tracking user identity; establishing mechanisms for auditing activity; establishing a means of verifying users; and establishing a means for restricting EPHI transmissions over an electronic network.

Law firms that handle EPHI for covered entities will need to adopt administrative safeguards such as developing policies and procedures, appointing a security officer, establishing sanctions for violations, providing regular training and perform regular evaluations of policy effectiveness.

On July 8, 2010, the Department of Health and Human Services (HHS) announced proposed regulations to implement the modifications to Privacy, Security and Enforcement rules under the HITECH Act.[52] HHS published the proposed rule on July 14, 2010.[53] The proposed rule added "subcontractors" to the definition of BAs so that subcontractors that provide services to a business associate and that require access to PHI would be considered a BA. As of the time this article went to press, HHS still had not issued a final rule.

Suggested Best Practices

Given the ethical and legal implications for lawyers who handle personal data provided by a client or produced by an adversary, particularly when there is a data breach involving that data, it is important to take immediate steps to help secure the data and protect against inadvertent disclosure. Some steps to consider:

- Minimize production of client personal information, financial information, and health information. Prior to production, ask whether the production of a Social Security number or other personal information is essential or whether the parties can reach agreement on the redaction of the personal information prior

to production. In most situations, the Social Security number is neither needed nor relevant to the underlying litigation.

- If production of personal information is unavoidable, consider entering an agreement with your adversary that provides for baseline security protections for the data and notice in the event of unauthorized access in the following manner:

  When confidential data is produced using data security measures the receiving party will implement the same or substantially equivalent data security measures when providing the information to others, such as its consultants, experts, and third-party vendors. By way of example, if a producing party designates electronically stored information (ESI) as confidential and produces it on encrypted disks, when providing the same ESI to its experts or consultants, the receiving party will produce the ESI on encrypted disks, or through an alternative measure providing data security substantially equivalent to the use of encrypted disks.

  If a receiving party becomes aware of any unauthorized access to confidential documents or ESI provided to it by a producing party, or has a reasonable belief that a substantial risk of unauthorized access exists, the receiving party will provide notice to the producing party as soon as practicable, which notice will be of sufficient detail to allow the producing party to determine whether it must or should notify others of such unauthorized access or risk thereof.

  This language will provide some comfort that your adversary is on notice that the data being produced is confidential, that the data must be protected, and that prompt notice must be given in the event of unauthorized access.

- When possible encrypt, encrypt, and encrypt. Encryption is a safe harbor under state data breach laws and greatly reduces, if not eliminates, the risk of a data breach.

- Maintain robust document disposal policies that, among other things, require crosscut shredding for paper records if those records are destroyed in house or certificates confirming sanitization and destruction if performed by outside vendors for electronic and paper data.

- Consider the following language regarding destruction of data produced to an adversary:

  Upon the earlier of (a) expiration of the applicable limitations period for legal malpractice claims, or (b) six years from the date of full and final resolution of this action via settlement or otherwise, counsel for the Parties will provide opposing counsel with an affidavit confirming that all paper documents, electronic media, and contents of electronic media produced by the opposing litigant(s) and designated as Confidential have been destroyed in accordance will the following procedures:

  (a) Any paper documents designated as Confidential (such as, by way of example, documents containing Social Security numbers, drivers license numbers, bank account numbers, credit card numbers, debit card numbers, or dates of birth) are to be crosscut shredded, burned, or pulverized in order to make such documents unreadable or undecipherable and unusable.

  (b) Electronic media, including computer hard drives, audio tapes, video tapes, floppy disks, DVDs and CDs designated as Confidential information should be completely sanitized prior to destruction so that all information contained in the electronic media is unreadable, undecipherable or impossible to practically reconstruct.

- Review policies and training regarding removal of personal information from the workplace.

- Pursuant to Rule 1.6, discuss with clients at the beginning of the engagement whether any special circumstances warrant protection of their data and what the best method of protection would be given the nature of the data.

- Reduce the number of documents that may contain client personal information left in printers or unsecure areas within the law firm.

- Adopt a comprehensive data breach incident response plan so that the law firm can respond to an incident efficiently and expeditiously.

- Carefully monitor third-party agreements with vendors and experts to ensure compliance with ongoing data security obligations.

- Adopt a written information security plan.
- Engage in frequent training of attorneys and support staff.
- Monitor technology to keep abreast of threats to confidentiality of client data.

As lawyers, we have ethical and legal obligations to maintain the security and confidentiality of client personal data. While no organization can ever be completely insulated from data breaches, it is particularly important that attorneys and law firms implement policies and procedures to enhance the protection of client data.

Notes

1. *http://calcoastnews.com/2010/10/confidential-prisoner-records-found-discarded-in-dumpster.*
2. *http://calcoastnews.com/2010/10/confidential-prisoner-records-found-discarded-in-dumpster.*
3. *http://www.imakenews.com/accushred/e_article001846709cfm?x=b11,0,w.*
4. *http://www.kens5.com/news/Private-information-dumped-near-Interstate-10-99438849.html.*
5. *http://www.kens5.com/news/Private-information-dumped-near-Interstate-10-99438849.html.*
6. *http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202473036068.*
7. *http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202473036068.*
8. *http://www.privacyrights.org/data-breach.*
9. *http://www.oag.state.md.us/idtheft/Breach%20Notices/ITU-157538.pdf.*
10. *http://www.law.com/jsp/article.jsp?id=1202426435623&slreturn=1&hbxlogin=1.*
11. *http://doj.nh.gov/consumer/breaches.html.*
12. *http://doj.nh.gov/consumer/pdf/alix_partners.pdf.*
13. *http://www.oag.state.md.us/idtheft/Breach%20Notices/ITU191412.pdf.*
14. *http://www.asc.state.al.us/Orders/2010/SC-2010-0016/Report%20on%20Document%20Release.pdf*, at p.4.
15. *http://www.asc.state.al.us/Orders/2010/SC-2010-0016/Report%20on%20Document%20Release.pdf*, at p. 8.
16. *http://www2.newsadvance.com/member-center/share-this/print/?content=ar162638.*
17. *http://doj.nh.gov/consumer/pdf/experian1.pdf.*
18. *http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf*, at p.2.
19. *http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf*, at p.33.
20. *http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf*, at p.33.
21. AR, AZ, CT, ID, IL, IN, IA, KY, ME, MD, MN, MS, NE, NH, NY, NC, ND, NM, OH, OK, PA, RI, SC, SD, TN, UT, VT, WA, WI.
22. In the Matter of Litz, Ind. Sup. Ct. Cause No. 55S00-1006-DI-325 (Shepard , C.J.) (Sept. 20, 2010).
23. *http://www.floridabar.org/tfb/TFBETOpin.nsf/b2b76d49e9fd64a5852570050067a7af/b3861cd80f9b3c0b852577f8006ea7cf!.*
24. *http://www.floridabar.org/tfb/TFBETOpin.nsf/b2b76d49e9fd64a5852570050067a7af/b3861cd80f9b3c0b852577f8006ea7cf!.*
25. *http://www.floridabar.org/tfb/TFBETOpin.nsf/b2b76d49e9fd64a5852570050067a7af/b3861cd80f9b3c0b852577f8006ea7cf!.*
26. *http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836*, Formal Opinion 2010-179.
27. *http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836*, Formal Opinion 2010-179.
28. *http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836*, Formal Opinion 2010-179.
29. Cal. Civ. Code § 1798.81.
30. Conn. Pub. Acts No. 08-167.
31. Mass Gen. L. ch. 931, § 1.
32. Mass Gen. L. ch. 931, at § 2.
33. Ind. Code § 24-4-14.
34. 201 CMR 17.03 (1).
35. 201 CMR 17, *et seq.*
36. 201 CMR 17.03 (2) (g).
37. Ark. Code Ann. § 4-110-104 (b);Ca. Civ. Code § 1798.81.5(b); Conn. Public Act 08-167; Md. Commercial Law Code Ann. §14-3503; Nev Rev. Stat 603A.210 R. I. Stat 11-49.2-2(2) and (3); Or. Rev. Stat. § 646A.622; Tex. Bus. & Comm. Code Ann. 48. 102(a); and Utah Code Ann. 13-44-20.
38. 201 CMR 17.04 (3) and (5).
39. Nev. Rev. Stat. § 603A.215 (1).
40. Nev. Rev. Stat. § 603A.215 (2).
41. Alaska (Alaska Stat. § 45.48.010 *et seq.*); Hawaii (HAW. REV. STAT. §§ 487N-1 to-4); Indiana (Ind. Code Ann. §§ 24-4.9-1-1 to 24-4.9-5-1 (2006) (business); § 24-4.9-2-2 as amended (2009)) ; Massachusetts (ALM GL CH 93H §§ 1, 3-6 (2007)); North Carolina (N.C. Gen. Stat. § 75-65) Wisconsin (Wis. Stat. § 134.98).
42. Recommended Practices on Notice of Security Breach Involving Personal Information, June 2009, *http://www.privacy.ca.gov/res/docs/pdf/COPP_Breach_Reco_Practices_6-09.pdf.*
43. Ct. Public Act No. 08-167.
44. Mich. Comp. Laws § 445.84 (2008).
45. N.M. Stat. § 57-12B-3(d); N.Y. Gen. Bus. Law § 399-dd (4).

46. Tex. Bus. & Com. Code § 501.052.
47. Engeseth v. County of Isanti, 665 F. Supp. 2d 1047 (D. Minn. 2009).
48. Allstate Insurance v. Linea Latina De Accidentes, Inc., Civ. No. 09-3681, 2010 U.S. Dist. LEXIS 124773, at *1-2 (D. Minn. Nov. 24, 2010).
49. *Id.* at * 8-9.
50. 45 C.F.R. § 160.103.
51. HITECH Act, Pub. L. No. 111-5 (Feb. 17, 2009) at § 13401(a).
52. *http://www.hhs.gov/news/press/2010pres/07/20100708c.html.*
53. 75 Fed. Reg. 134, 40868 (Jul. 14, 2010).