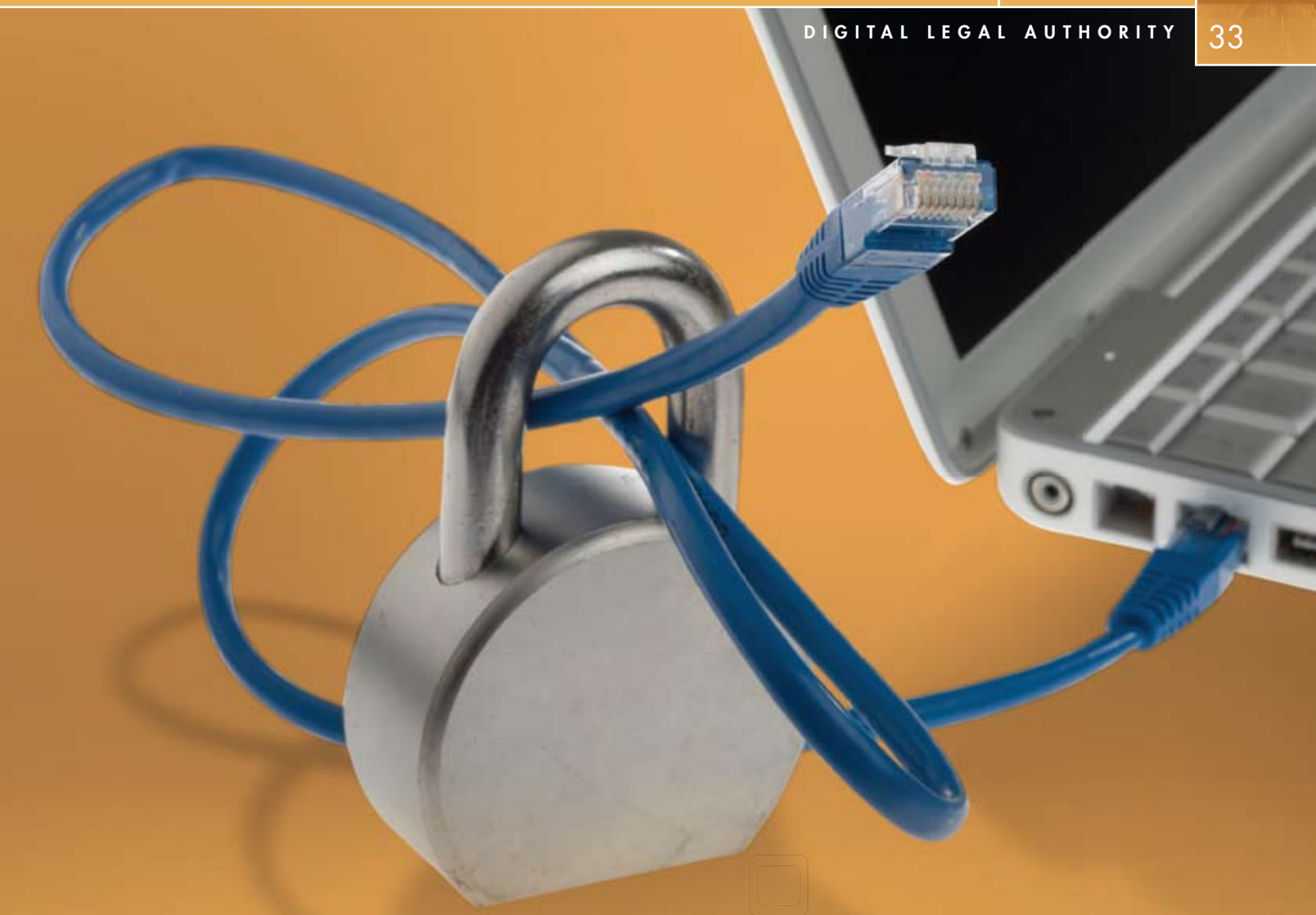


Data Privacy in the Law Firm

How to Protect Client Data

By Faith M. Heikkila

Fast Facts

Law firms must comply with their clients' regulatory compliance requirements and safeguard client data, especially personally identifiable information (PII).

Michigan is one of 44 states with data security breach notification laws regarding PII that law firms must comply with; these laws are applicable based on where the client resides rather than where the data resides.

It is critical to monitor where PII is stored, who is authorized to have access, who has custody of it, and whether it is encrypted.

Traditionally, law firms have protected client files in paper format. But what about electronic files in offsite storage or stored on a network, backup tapes, laptops, and removable media devices such as USB flash drives or CDs? How are those safeguarded? With the pervasiveness of electronically stored information, a new paradigm of providing data privacy protections has emerged. Clients are asking their lawyers to produce the firm's written comprehensive information security management plan in accordance with the clients' applicable regulatory compliance requirements. Law firms have clients who must comply with regulations like the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act, and the Payment Card Industry Data Security Standards, to name a few. When protected data is transferred to the law firm by the client, the law firm must also comply with these regulations and provide adequate safeguards.[1]

Lawyers also have an ethical obligation to protect confidential client data, including data retained in electronic format on a network connected to the Internet.[2] For example, while prepping for a deposition, you download onto your laptop client confidential information that includes the personally identifiable information (PII) or personal information of your client's customers. On the way home, you stop at a restaurant to meet friends and leave your laptop in the backseat of your car, only to discover later that the laptop was stolen while you were inside the restaurant. Unfortunately, the laptop data was not encrypted. Another example is transferring employee PII from the law firm's network to an unencrypted CD, DVD, or USB flash drive and losing this removable media device.[3] A third consideration is not knowing that lawyers, paralegals, or other staff are e-mailing PII or client confidential information to accounts outside of the law firm's network (or allowing it to happen), which may compromise the data because the firm does not directly control those e-mail accounts.

In each of these security breach examples, under Michigan Senate Bill 309, you must inform the parties involved that their PII has been compromised. The Michigan data security breach notification law became effective on July 2, 2007.[4] Pursuant to this statute, the triggers for notifying clients of a PII breach by individuals, businesses, state agencies, or agencies that own or license data include access and acquisition by an unauthorized person to unencrypted or unredacted computerized data or to encrypted data (with unauthorized access to the encryption key).[5] Parties who must be notified of the breach include individuals whose PII was compromised and credit reporting agencies if more than 1,000 individuals were affected. The penalty is $250 for each failure to provide notice, with an aggregate liability not to exceed $750,000.[6]

If you have clients who produce their customer data from other states, those states' data breach notification laws are applicable based on where the customer resides rather than where the company does business or where the breach occurred.[7] As of May 2009, 44 states (excluding Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota), the District of Columbia, Puerto Rico, and the Virgin Islands[8] pattern their laws after the 2003 California Senate Bill 1386 and require that affected individuals be notified in the event that PII is exposed to unauthorized parties.[9]

PII is primarily defined as pieces of computerized data that can be used to distinguish or trace an individual's identity. In Michigan, this data includes a person's first name or first initial along with last name used in conjunction with:[10]

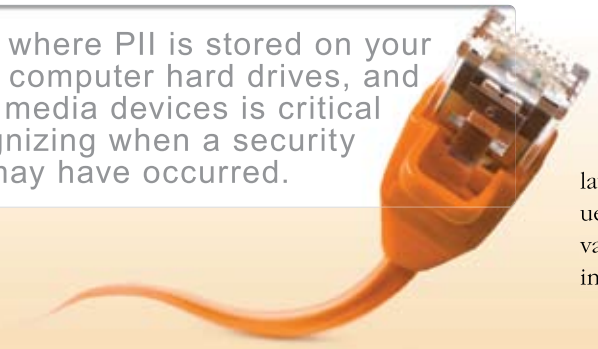
- Address and telephone number
- Driver's license or state personal identification card number
- Social Security Number (SSN)
- Place of employment
- Employee identification number
- Employer or taxpayer identification number
- Government passport number
- Health insurance identification number
- Mother's maiden name
- Demand deposit account number
- Savings account number
- Financial transaction device account number or the individual's account password
- Stock or other security certificate or account number
- Credit card account number
- Vital record
- Medical records or information

Additionally, personal information of a Michigan resident includes an individual's first name or first initial along with last name linked to one or more of the following:[11]

- SSN
- Driver's license or state personal identification card number
- Demand deposit or other financial account number, or credit card or debit card number in conjunction with any required security code, access code, or password that would permit access to any of the individual's financial accounts

Protecting client data and PII can be a very daunting task for law firms as the proliferation of portable media devices continues to increase and the pervasive nature of saving data on a wide variety of computers and devices becomes more prevalent. Knowing where PII is stored on your network, computer hard drives,

Knowing where PII is stored on your network, computer hard drives, and portable media devices is critical for recognizing when a security breach may have occurred.



and portable media devices is critical for recognizing when a security breach may have occurred. See the "Checklist for Monitoring Where PII or Personal Information is Stored" on page 36 for help with monitoring the location of PII and personal information collected pursuant to the Michigan data security breach notification law.

Best Practice Tips for Preventing Unauthorized Access to Client Data and PII

The following best practice tips are not an exhaustive list, but are critical ones to consider when protecting a law firm's confidential and sensitive client information as well as employee PII.

- Encrypt PII when it is in transit or at rest on computer hard drives or servers, even if it is not mandated by law. Ensure that the information is securely protected even when at rest on the network.[12]
- Install technical controls such as firewalls, anti-virus software, and anti-spyware on the firm's network to protect the data at rest on the firm's servers and computers. Consider installing data leakage protection software to prevent data leakage and to monitor what data leaves the confines of the firm. Also, consider using an intrusion detection system and intrusion protection system technology to help detect and protect PII from being compromised.
- Be knowledgeable about the requirements of applicable data privacy protection laws and regulations.
- Start building an information security management program by designating one person to be in charge of security in your firm and regularly reporting results to your managing partners.
- Develop information security policies, including one that covers acceptable use of the computers and client data, as well as controls for accessing data. In addition to physical controls, such as locks, alarms, or cameras, use strong passwords and multifactor authentication devices that require a second tier of identification to protect sensitive client data.
- Develop, implement, and test your data breach response plan regularly to ensure it is current and effective. Create awareness and incentive programs for employees to report a data breach incident.
- Properly train all custodians of PII on the best practices of protecting this data while in their possession and on the appropriate use of critical assets.
- Conduct regular risk assessments to identify where and how your firm stores or transmits PII.
- Collect only the PII your law firm needs to conduct business with the client. Ensure this collected PII is protected by allowing access only to those who require it to complete their jobs and the firm's transactions. Create a policy restricting the removal of PII from the firm without appropriate encryption in place.

A sledge hammer, power drill, or magnet can be extremely helpful when it comes to properly disposing of hard drives containing information.

- Being in possession of PII does not give you authority to transfer it to a third party. This type of data should not be shared with third parties unless there is a business use necessary for disclosure of PII to complete a business transaction. There should also be a contract outlining how third parties will protect this information while it is in their custody. A vendor management program should be implemented to ensure that the shared data is being adequately protected by appropriate security measures while in the third party's possession.
- Destroy sensitive data when it is no longer needed. Never dispose of PII in a public receptacle or in your own personal garbage without first shredding it with a cross-strip shredder. Immediate use of a cross-strip shredder that pulverizes the paper into unreadable form is best rather than relying on a service to shred it. This includes the secure wiping of all hard drives and servers before reissuing them or disposing of them. Pulverize, burn, or shred hard drives as well as paper documents. A sledge hammer, power drill, or magnet can be extremely helpful when it comes to properly disposing of hard drives containing information.
- Develop, review, and assess your information security management program, policies, and procedures to ensure they are current and effectively communicated throughout your law firm. An assessment by an independent information security firm is not only a good business practice, but is often required by your clients and data privacy regulations. ■

Faith M. Heikkila, CIPP, is Pivot Group's regional security services manager in Kalamazoo with research interests in information security policies and procedures, privacy issues, e-discovery, and security breaches. She has more than 18 years of paralegal and IT project management experience. Faith anticipates a 2009 completion date of her PhD in information systems concentrating in information assurance at Nova Southeastern University. Contact her at fheikkila@pivotgroup.net.

Checklist for Monitoring Where PII or Personal Information is Stored

PII OR PERSONAL INFORMATION TYPE IN COMBINATION WITH FIRST NAME OR FIRST INITIAL AND LAST NAME	ENCRYPTION		LOCATION								
	ENCRYPTED	ENCRYPTION KEY NOT WITH DATA	DO NOT COLLECT	NETWORK	LAPTOP	USB DRIVE	E-MAIL	BLACKBERRY OR PDA	CELL PHONE	COMPUTER HARD DRIVE	CD OR DVD
Address and telephone number (by itself it is not considered a breach because of its availability in public records)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Driver's license or state personal identification card number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Social Security Number (SSN)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Place of employment	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Employee identification number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Employer or taxpayer identification number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Government passport number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Health insurance identification number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Mother's maiden name	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Demand deposit account number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Savings account number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Financial transaction device account number or the individual's account password	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Stock or other security certificate or account number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Credit card account number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Vital record	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Medical records or information	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Demand deposit or other financial account number, or credit card or debit card number in conjunction with any required security code, access code, or password that would permit access to any of the individual's financial accounts	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒

FOOTNOTES

1. Comerford, *Competent computing: A lawyer's ethical duty to safeguard confidentiality,* 19 Geo J Legal Ethics 629 (2006).
2. *Id.*
3. Heikkila, *Encryption: Security considerations for portable media devices,* 5 IEEE Security & Privacy 22 (July/August 2007).
4. MCL 445.72; see also Kugele & Placer, *Navigating some uncertain waters in Michigan's new security breach notification law,* Privacy & Data Security L J 710 (July 2007).
5. MCL 445.72(1)(a) through MCL 445.72(1)(b).
6. MCL 445.72(12) through MCL 445.72(14).
7. Schwartz & Janger, *Notification of data security breaches,* 105 Mich L R 913 (2007).
8. National Conference of State Legislatures, *State Security Breach Notification Laws* <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm> (accessed June 15, 2009).
9. Silverman, *Data security breaches: The state of notification laws,* 19 J Intell Prop & Tech L 5 (2007).
10. MCL 445.63(o).
11. MCL 445.63(e) and MCL 445.63(p).
12. Heikkila, n 2 *supra.*