Policies and Processes for **Protecting Information**

Though written primarily for a law firm audience, this article provides all organizations with practical advice about protecting personal, confidential, and trade secret information. It is an excerpt from *Confidentiality, Privacy, and Information Security: A Primer for Law Firm Records and Information Governance Professionals*, written by Beth Chiaiese, CRM, with Lee. R. Nem-chek, IGP, CRM, editor for the Information Governance in the Legal Environment series.

Beth Chiaiese, CRM

Best practice dictates that law firms must use a variety of tools and techniques to secure Covered Information in their possession. [*Editor's note:* Throughout this excerpt, the term "Covered Information" refers to all private or confidential law firm information that is regulated by ethics rules, data privacy and security laws, or common law.] These include implementing a strong security infrastructure for the firm's network, developing robust policies, using specific procedures and systems designed to minimize the risks of a data loss, and auditing to identify gaps in compliance with the established policies and procedures. [This excerpt focuses on policies and processes.]

… the underlying message regarding information security should be that the firm expects all personnel to manage information in ways that support compliance…

Policies

A significant component of a law firm's IG [information governance] framework consists of guidance on information confidentiality, privacy, and security. Some IG policies relate narrowly to information security. Others include statements related to the protection of Covered Information but also cover topics such as records management, legal holds, and accepting and releasing client information.

Regardless of the specific objective of a policy, the underlying message regarding information security should be that the firm expects all personnel to manage information in ways that support compliance with professional duties of confidentiality, relevant regulations that govern the use of PI, and requirements to protect intellectual property and trade secrets.

The section below discusses specific policies that a firm can adopt within an overall IG policy framework to strengthen its information security program. Many firms require new personnel to acknowledge receipt, read, and agree to the provisions of such policies on their first day of employment, and they may also require annual re-certification by all personnel.

Confidentiality Policy

A statement of the firm's requirements to maintain the confidentiality of client and firm information is a threshold compliance policy in most law firms. Many law firm liability insurance providers strongly recommend that firms enforce this type of policy. Firms generally place so much importance on maintaining confidentiality that violations can result in severe discipline, including dismissal from employment. Recommended policy elements include:

- Definition of confidential information
- Scope statement defining the policy as covering all client and business confidential information, regardless of format, media, storage location, or method of transmission
- Statement regarding consequences of non-compliance
- Specific requirements to protect oral, written, electronic, and physical confidential information
- Permitted use, access, and disclosure of confidential information
- Transmittal protocols for confidential information, including any requirements to encrypt data in motion
- Guidelines in the event of the inadvertent disclosure of confidential information
- Securing confidential information from guests
- Retention and disposal of confidential information

Information Security Policy

A firm's information security policy should set forth expectations regarding how firm personnel must secure Covered Information. Some firms may also wish to excerpt a brief statement of their expectations regarding information security that can be given to clients and third parties.

The information security policy is a good vehicle to include requirements for password control, although some firms create separate password policies. In addition, some firms create broader "technology acceptable use" policies that incorporate information security requirements.

Recommended elements for general information security policies include:

- Password and authentication requirements
- Securing confidential matters and matters under ethics walls
- Securing confidential documents
- Encrypting information in transit
- Appropriate use of portable devices, including device encryption
- Rules for participation in the firm's BYOD program
- Permissible uses of the Internet
- Permissible use of social media and networking sites
- Use of public cloud storage services
- Securing physical information

BYOD Policies

While policies governing participation in a firm's BYOD program might be included in a general information security policy, best practice dictates that firms require program participants to sign a separate [BYOD] agreement, certifying that they understand the parameters of the program and their responsibilities, including a requirement to re-certify annually. Other recommended elements of the agreement include:

- Program definition and scope
- Eligibility statement
- Provision detailing the types of devices that are and are not covered by the program
- Requirements regarding virus protection and encryption
- Requirements regarding temporary and permanent storage of client and firm information
- Description of how the firm ensures connectivity to firm systems
- Requirements that the participant is responsible for software and hardware maintenance
- Financial reimbursement processes

> …best practice dictates that firms require program participants to sign a separate [BYOD] agreement, certifying that they understand the parameters of the program and their responsibilities…

Policy on Managing Personal Information

A policy providing guidance on the management of PI [personal information] should include the following elements:

- Definition of PI
- Approved locations for storing PI
- Approved methods of securing PI
- Permitted access, use, and disclosure of PI
- Notification of a PI breach
- Requirements for use of a BAA [business associate agreement]
- Release or transmission of PI
- Retention of PI
- Destruction of PI

Social Media and Networking Policy

Lawyers and non-lawyer firm personnel alike engage in social networking both professionally and personally. Law firms have an interest in ensuring that such interactions comply with professional duties, regulatory requirements, and firm policies. Although there are personal privacy considerations that prohibit firms from dictating how employees use social media in their personal lives, professional obligations covering the behavior of lawyers are in force at all times. This means that lawyers cannot identify their clients or divulge any confidential client information while using social media.

Social networking policies typically include provisions dealing with a variety of professional responsibility and legal issues that extend beyond confidentiality and security. These issues include (1) prohibitions against providing legal advice while using social media; (2) using disclaimers to advise readers not to interpret content as legal advice; (3) complying with copyright and trademark laws; (4) complying with lawyer advertising rules; (5) posting content in an objective and factual manner; (6) refraining from expressing defamatory opinions about individuals; and (7) not using social networking to seek input on candidates for firm employment.

Certain elements of such policies touch directly on privacy and confidentiality, including:

- Prohibitions against discussing firm business and professional relationships with clients, judges, and other lawyers
- Prohibitions against using social media to discuss legal matters with clients
- Requirements to be transparent and not to use misleading language or pretext
- Requirements to protect the privacy of others

Processes and Systems

The ability of firm personnel to comply with mandated policies depends on a number of strong processes, systems, and associated tools. This monograph does not cover all of these in depth, but several significant components of law firm information security programs are discussed below.

Approved Repositories

As noted earlier, a contributing factor to data loss in law firms is the dispersion of Covered Information across multiple repositories. Increasingly, law firms attempt to aggregate information into approved locations in order to better manage the information from a security standpoint. Each approved repository in the firm should share certain common characteristics. Approved recordkeeping repositories in a law firm must be able to:

- Classify information by a common identifier, such as a client/matter number
- Preserve information for a prescribed period in the event of a lawsuit, claim, or investigation, or as part of a record "declaration" process (in order to prevent further modification)
- Secure information from access by unauthorized individuals
- Permanently delete/destroy information in accordance with policy,

agreement, or court order

Firms can identify approved and non-approved repositories using these characteristics as defining guidelines. For example, most DMS [document management system] products can function as approved repositories, as can a physical file folder. E-mail systems, on the other hand, cannot, because, although e-mail boxes are private to the individual user and e-mail can be permanently destroyed, e-mail systems per se do not support classification or preservation.

- Integration with multiple firm information systems—e.g., DMS, RMS [records management system], docket systems, and time-entry systems—thus allowing consistent security across systems
- Alerts to system administrators that a non-authorized individual is trying to gain access to a confidential matter
- Monitoring of the time-keeping system for individuals who have billed time to confidential matters, and either alerting the system administrator if the individual is also working on the opposite side of the wall or automatically adding the individual to the wall
- Allowing the system administrator to grant end-user capability to manage access; for example, if all matters for a client are considered confidential, it may be helpful for the relationship partner's assistant to manage access. Alternatively, the office of the General Counsel may want to manage security for all firm legal matters.
- Restricting or allowing access by group; for example, based on the area of law code assigned to a matter (e.g., health care or employee benefits), it is possible to grant access to matters containing PHI [personal health information] to only a defined group of lawyers and staff. Similarly, it is possible to create a group of foreign nationals and restrict them from accessing matters that contain information covered by ITAR [The International Traffic in Arms Regulations] / EAR [Export Administration Regulations].
- Reporting on all confidentiality walls in the firm, as well as the walls on which individual lawyers or staff are named
- Auditing capability to monitor spikes in downloading and e-mailing activity

As noted above, confidentiality software assists users to comply with the requirements of certain DSP [data security and privacy] laws. To facilitate this assistance, some firms ask at matter intake if the new matter requires the receipt of PI or PHI. If yes, a confidentiality wall can be created.

… most DMS [document management system] products can function as approved repositories, as can a physical file folder. E-mail systems, on the other hand, cannot …

Securing Matters from Unauthorized Access

Software is available that secures all content related to one or more matters for a client. Matter level security can be configured to be either exclusionary or inclusionary. Exclusionary security applies when specific individuals are excluded from access. Typically, this occurs when an ethics wall is required to screen lawyers or others who have confidential information related to the client or matter that could result in the firm's disqualification. [States vary in their recognition of ethics walls as effective screens against conflicts imputation. Records managers and IG professionals are encouraged to consult with their firm's professional responsibility lawyer regarding the appropriate use of ethics walls.]

Inclusionary security is applied when *only* specific individuals are permitted access to the subject information. This generally occurs when the matter itself is confidential, such as merger and acquisition matters, criminal matters, family law, and other highly personal client matters.

Confidentiality software should include the following functionality:

Document Level Security

DMS systems include functionality that defines access parameters at the document level.

Defining Access Rights – In general, law firms maintain "optimistic" or "open" DMS environments. This means that the default security setting for documents is public, i.e., all documents are accessible by everyone in the firm. Document authors can change this setting to "read only," which allows everyone to view the document, but only the author and other approved users are permitted to modify it.

Alternatively, authors can change the setting to "private," which means that no one other than the author and other approved users can view and/or modify the document. Because this level of security is controlled by the end user, it requires awareness, skill, and accountability on the part of all firm personnel. Thus, it is a significant component of the firm's security training program.

Tagging by Document Type – Most DMS applications allow system administrators to configure specific document types to default as private to the author, which makes it easier to set security at the document level. The author can grant access to others as appropriate. Examples include the document types Personnel, Personal, and Firm Management. An alternate approach is to create a document type called PI or PHI, which satisfies the requirements of certain DSP laws that require organizations in possession of PI to take affirmative steps to control access to it.

Encryption

Encryption is accomplished by using software to apply a complex series of mathematical algorithms on data to convert it to cipher text. The more complex the algorithm, the more difficult it is to decrypt the data. Although a complete technical description of encryption is beyond the scope of this monograph, law firm records and IG professionals must understand certain key concepts about encryption.

Encrypting Data in Transit – Individual data sets (documents or e-mails) can be encrypted at the time of transmission. In such instances, software applied by the sender translates plain text into cipher text. The recipient needs a key (i.e., a password) to decrypt the data to make it readable. Users must encrypt PI before e-mailing or otherwise transmitting it electronically. Passwords should always be communicated orally; do not send them in plain text via e-mail or facsimile.

Encrypting Data at Rest – Encryption can be applied to an entire hard drive, and a password is needed to decrypt the drive. The advantage of this approach is that if a strong password is used, it is almost impossible for an unauthorized user to access data on the hard drive. The disadvantage is that if the password is broken, the entire hard drive is decrypted when the password is entered. This consequence further supports the necessity to create complex, hard to crack passwords.

Many firms automatically encrypt the hard drives of firm-owned laptops. Increasingly, they are also requiring users to encrypt the hard drives of personal devices, although several factors constrain such policies:

- *Some devices do not support encryption.* Firms can address this issue by specifying the types of devices that can be encrypted and giving individuals a time period within which to migrate. In addition, the firm's BYOD policy can limit the types of devices for which the firm will provide reimbursement to only those that support encryption.
- *Firms have limited capabilities to monitor personal devices.* Because certain applications can be accessed directly over the Internet, or because individuals might e-mail documents to personal e-mail accounts or store them on portable media such as thumb drives, firms cannot entirely con-

trol whether Covered Information is stored on encrypted devices.

- *Installing encryption software can be technically challenging*. On certain devices, encrypting the hard drive is as simple as enabling a feature in the operating system or securing it with a password. Other devices require the installation of encryption software. Law firms that mandate encryption of personal devices should be prepared to assist individuals who do not have the skill to do it on their own.

Examine any portable media on which electronic information resides to confirm that it is not infected with a virus or malware.

File Transfer Protocols

As noted earlier, movement of confidential client information has become an operationalized component of RIM and IG programs. Whereas law firms have had processes to manage physical file transfers for many years, these processes must now include the ingestion or release of significant amounts of electronic information. File transfer methods were explored in depth in the second monograph of this series [*Lawyer and Matter Mobility*]. With respect to information security, however, the following additional considerations apply:

Ingestion of Information – When receiving physical and electronic records from an outside source, such as a client or former law firm, confirm the following:

- The current firm has been engaged by the client and is thus permitted to have the information. This can be accomplished by receiving an e-mail confirmation from the client, by obtaining a copy of the written consent from the former firm to release records to the current firm, or by executing an engagement agreement with the client. If none of these conditions exist, do not examine or review the information until the client's intent has been documented, to avoid inadvertently accessing privileged or otherwise confidential information.
- Examine any portable media on which electronic information resides to confirm that it is not infected with a virus or malware.
- Load electronic data onto a review site that is not connected to the network, allowing further examination to identify viruses. In addition, this allows staff managing the transfer to organize and aggregate data by appropriate client and matter and provides a location for lawyers to access information while the transfer proceeds. Finally, it allows file transfer staff an opportunity to further examine data to remove records for clients who have not engaged the firm and inadvertently transmitted trade secret information from the former firm.
- After data has been thoroughly examined, client engagement has been confirmed, and client/matter numbers have been issued, the data can be loaded into firm systems on the network.

Release of Information – When information is released from the firm, take precautions to avoid the inadvertent disclosure of confidential client information, a breach of PI, or the potential release of firm trade secrets:

- Release information only after an appropriate analysis to determine the firm's potential need to review the file to remove records necessary to defend the firm. This analysis should be done by a loss prevention or professional responsibility lawyer or by the firm's General Counsel.
- Follow firm guidelines for the removal of firm trade secret information from the file.
- Encrypt any PI or PHI before transmission to the receiving party.
- Appropriately secure physical files prior to shipping.
- Use an FTP site or other secured means to transmit electronic records. If using portable media, such as a CD or DVD, confirm that it is virus-free.
- If shipping physical files or portable media, use a courier or other traceable method.

Collaboration Systems

Lawyers are increasingly downloading inexpensive or free solutions from the Internet to share information and collaborate with clients and other parties. To combat this risky behavior, firms are either developing internal solutions that provide the same functionality within the firm's security architecture, or they are implementing commercial solutions that meet the firm's security requirements.

Mobile Device Management (MDM)

A number of services impose centralized control over mobile devices that connect to firm networks. Common features of MDM systems include [according to Sharon D. Nelson, David G. Ries, and John W. Simek in *Locked Down: Information Security for Law Firms]*:

- *Inventory control* – Once a device, such as a smartphone, tablet, or laptop, connects to firm networks, the MDM system uses its IP address to track it, ensuring that users are relying on devices that support firm guidelines regarding encryption. Inventory control also allows the firm to monitor devices that have been inactive for a specified period so they can be wiped of firm data and removed from the network.

- *Connectivity management* – Examples include deploying secured virtual private networks (VPN) or wireless networks that allow users to gain remote entry to firm systems.
- *Password management* – This includes protocols to require regular password changes and system authentication.
- *Remote wiping of lost or stolen devices* – Although remote wiping is a critical aspect of mitigating data breach risks, it also endangers personal data on the device, as noted earlier. In addition, the firm's ability to wipe the device depends on a user's notification that his device was lost or stolen.
- *Timing out* – After periods of inactivity, password re-entry is required.
- *Remote installation* – Applications and updates can be installed wherever the device is being used.

Removal or Restriction of Administrative Rights

Firms can restrict the ability of users to access certain administrative rights in the operating systems of their networks, including the ability to install software and devices. Although partners may push back heavily on this restriction, IT and IG leaders should not back down. Not only does the restriction of administrative rights ensure that only firm-approved systems are in place, it can prevent the inadvertent entry of viruses and other malware into the firm's environment, either through direct download by firm personnel or by social engineering manipulation.

Secure Disposal

Many DSP laws require secure methods of records disposal. In addition, secure disposal prevents leaking other types of Covered Information, including confidential client PI and trade secrets. Records managers are well-acquainted with secure methods of disposing of hard copy records, including cross-cut shredding and pulping. However, securely disposing of electronic records is more complex. Pressing the Delete key removes the pointers that allow data to be accessed, but it does not expunge data from the hard drive on which it is written.

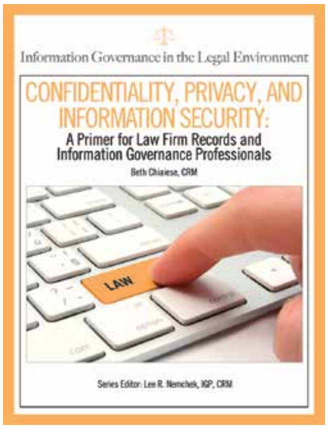
Acceptable methods to dispose of electronic information include the following [according to Nelson, Ries, and Simek]:

- Physically destroying the drive or portable media on which the data is written by disintegration, pulverization, incineration, or shredding
- Degaussing, "a magnetic process by which magnetic media are erased (returned to zero) by applying a reverse magnetic field using a degausser"
- Overwriting the media with a disk-wiping program. Such applications overwrite each block or segment on the disk several times to obliterate the data.
- Encryption. If a device is securely encrypted, the data is not accessible unless it is unlocked with a password or key. If the device has strong encryption it can be disposed of using one of the methods listed above without otherwise sanitizing the device.

Culture

As with the IG program as a whole, the success of any law firm's information security program is dependent on building a culture of awareness, accountability, and compliance. Support from firm leadership and ongoing training are important contributing factors to making information security an accepted and followed protocol throughout the law firm. **END**

Beth Chiaiese, CRM, is the director of professional responsibility & compliance for Foley & Lardner LLP. She can be contacted at bchiaiese@foley.com. *See her bio on page 47.*


Information Governance in the Legal Environment
CONFIDENTIALITY, PRIVACY, AND INFORMATION SECURITY:
A Primer for Law Firm Records and Information Governance Professionals
Beth Chiaiese, CRM
LAW
Series Editor: Lee R. Nemchek, IGP, CRM