PROFESSIONAL ETHICS OF THE FLORIDA BAR

OPINION 10-2
September 24, 2010

A lawyer who chooses to use Devices that contain Storage Media such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition, including: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

RPC: 4-1.1, 4-1.6(a), 4-5.3(b)

The Professional Ethics Committee has been asked by the Florida Bar Board of Governors to write an opinion addressing the ethical obligations of lawyers regarding information stored on hard drives. An increasing number of devices such as computers, printers, copiers, scanners, cellular phones, personal digital assistants ("PDA's"), flash drives, memory sticks, facsimile machines and other electronic or digital devices (collectively, "Devices") now contain hard drives or other data storage media[1] (collectively "Hard Drives" or "Storage Media") that can store information.[2] Because many lawyers use these Devices to assist in the practice of law and in doing so intentionally and unintentionally store their clients' information on these Devices, it is important for lawyers to recognize that the ability of the Devices to store information may present potential ethical problems for lawyers.

For example, when a lawyer copies a document using a photocopier that contains a hard drive, the document is converted into a file that is stored on the copier's hard drive. This document usually remains on the hard drive until it is overwritten or deleted. The lawyer may choose to later sell the photocopier or return it to a

leasing company. Disposal of the device without first removing the information can result in the inadvertent disclosure of confidential information.

Duty of Confidentiality

Lawyers have an ethical obligation to protect information relating to the representation of a client. Rule 4-1.6(a) of the Rules Regulating the Florida Bar addresses the duty of confidentiality and states:

> **(a) Consent Required to Reveal Information.** A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent.
>
> The comment to the rule further states:
>
> The confidentiality rule applies not merely to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or by law.

A lawyer must ensure confidentiality by taking reasonable steps to protect all confidential information under the lawyer's control. Those reasonable steps include identifying areas where confidential information could be potentially exposed. Rule 4-1.1 addresses a lawyer's duty of competence:

> **Competence** A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.
>
> The comment to the rule further elaborates:
>
> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law *and its practice*, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject.
>
> (emphasis added).

If a lawyer chooses to use these Devices that contain Storage Media, the lawyer has a duty to keep abreast of changes in technology to the extent that the lawyer can identify potential threats to maintaining confidentiality. The lawyer must learn such details as whether the Device has the ability to store confidential information, whether the information can be accessed by unauthorized parties, and who can potentially have access to the information. The lawyer must also be aware of different environments in which confidential information is exposed such as public copy centers, hotel business centers, and home offices. The lawyer should obtain enough information to know when to seek protection and what Devices must be sanitized, or cleared of all confidential information, before disposal or other disposition. Therefore, the duty of competence extends from the receipt, i.e., when the lawyer obtains control of the Device, through the Device's life cycle, and until disposition of the Device, including after it leaves the control of the lawyer. Further, while legal matters are beyond the scope of an ethics opinion, a lawyer should be aware that depending on the nature of the information, misuse of these Devices could result in inadvertent violation of state and federal statutes governing the disclosure of sensitive personal information such as medical records, social security numbers, criminal arrest records, etc.

Duty to Supervise

The lawyer must regulate not only the lawyer's own conduct but must take reasonable steps to ensure that all nonlawyers over whom the lawyer has supervisory responsibility adhere to the duty of confidentiality as well. Rule 4-5.3(b) states:

> **(b) Supervisory Responsibility.** With respect to a nonlawyer employed or retained by or associated with a lawyer or an authorized business entity as defined elsewhere in these Rules Regulating The Florida Bar:
>
> > (1) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
> > (2) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

> (3) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> > (A) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
> > (B) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

A lawyer's supervisory responsibility extends not only to the lawyer's own employees but over entities outside the lawyer's firm with whom the lawyer contracts to assist in the care and maintenance of the Devices in the lawyer's control. If a nonlawyer will have access to confidential information, the lawyer must obtain adequate assurances from the nonlawyer that confidentiality of the information will be maintained.

Sanitization

A lawyer has a duty to obtain adequate assurances that the Device has been stripped of all confidential information before disposition of the Device. If a vendor or other service provider is involved in the sanitization of the Device, such as at the termination of a lease agreement or upon sale of the Device, it is not sufficient to merely obtain an agreement that the vendor will sanitize the Device upon sale or turn back of the Device. The lawyer has an affirmative obligation to ascertain that the sanitization has been accomplished, whether by some type of meaningful confirmation, by having the sanitization occur at the lawyer's office, or by other similar means.

Further, a lawyer should use care when using Devices in public places such as at copy centers, hotel business centers, and outside offices where the lawyer and those under the lawyer's supervision have little or no control. In such situations, the lawyer should inquire and determine whether use of such Devices would preserve confidentiality under these rules.

In conclusion, when a lawyer chooses to use Devices that contain Storage Media,

the lawyer must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition. These reasonable steps include: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

---

1. As used in this opinion, Storage Media is any media that stores digital representations of documents.

2. See Brian Smithson, *The IEEE 2600 Series: An Introduction to New Security Standards for Hardcopy* Devices, **ISSA Journal**, Nov. 2009, at 28; Holly Herman, *Experts Warn Copiers Can Be Fertile Ground for ID Thieves*, **Reading Eagle** (Jun. 2, 2010, 12:28:54 P.M.), http://readingeagle.com/article.aspx?id=222523; Mark Huffman, *Digital Copiers Could Be an Identity Theft Threat*, ConsumerAffairs.com (May 19, 2010), http://www.consumeraffairs.com/news04/2010/05/digital_copiers.html; Armen Keteyian, *Digital Photocopiers Loaded with Secrets*, CBSNews.com (April 15, 2010), http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml; Gregg Kelzer, *Photocopiers: The Newest ID Theft Threat*, **Computerworld** (March 14, 2007), http://www.computerworld.com/s/article/9013104/Photocopiers_The_newest_ID_theft_threat.

[Revised: 12-13-2010]