___ N.J.L.J. ___

___ N.J.L. ___

Advisory Committee on Professional Ethics

Appointed by the Supreme Court of New Jersey

Opinion 701
Advisory Committee on Professional Ethics

Electronic Storage And Access of Client Files

The inquirer asks whether the Rules of Professional Conduct permit him to make use of an electronic filing system whereby all documents received in his office are scanned into a digitized format such as Portable Data Format ("PDF"). These documents can then be sent by email, and as the inquirer notes, "can be retrieved by me at any time from any location in the world." The inquirer notes that certain documents that by their nature require retention of original hardcopy, such as wills, and deeds, would be physically maintained in a separate file.

In Opinion 692, we set forth our interpretation of the term "property of the client" for purposes of *RPC* 1.15, which then triggers the obligation of a lawyer to safeguard that property for the client. "Original wills, trusts, deeds, executed contracts, corporate bylaws and minutes are but a few examples of documents which constitute client property." 163 *N.J.L.J.* 220, 221 (January 15, 2001) and 10 *N.J.L.* 154 (January 22, 2001). Such documents cannot be preserved within the meaning of *RPC* 1.15 merely by digitizing them in electronic form, and we do not understand the inquirer to suggest otherwise, since he acknowledges his obligation to maintain the originals of such documents in a separate file.

On the other hand, we also noted in Opinion 692 that a client file will likely contain other documents, such as correspondence, pleadings, memoranda, and briefs, that are not "property of the

client" within the meaning of *RPC* 1.15, but that a lawyer is nevertheless required to maintain at least for some period of time in order to discharge the duties contained in *RPC* 1.1 (Competence) and *RPC* 1.4 (Communication), among others. While traditionally a client file has been maintained through paper records, there is nothing in the RPCs that mandates a particular medium of archiving such documents. The paramount consideration is the ability to represent the client competently, and given the advances of technology, a lawyer's ability to discharge those duties may very well be enhanced by having client documents available in an electronic form that can be transmitted to him instantaneously through the Internet. We also note the recent phenomenon of making client documents available to the client through a secure website. This also has the potential of enhancing communications between lawyer and client, and promotes the values embraced in *RPC* 1.4.

With the exception of "property of the client" within the meaning of *RPC* 1.15, therefore, and with the important caveat we express below regarding confidentiality, we believe that nothing in the RPCs prevents a lawyer from archiving a client's file through use of an electronic medium such as PDF files or similar formats. The polestar is the obligation of the lawyer to engage in the representation competently, and to communicate adequately with the client and others. To the extent that new technology now enhances the ability to fulfill those obligations, it is a welcome development.

This inquiry, however, raises another ethical issue that we must address. As the inquirer notes, the benefit of digitizing documents in electronic form is that they "can be retrieved by me at any time from any location in the world." This raises the possibility, however, that they could also be retrieved by other persons as well, and the problems of unauthorized access to electronic platforms and media (i.e. the problems posed by "hackers") are matters of common knowledge. The availability of sensitive client documents in an electronic medium that could be accessed or intercepted by unauthorized users therefore raises issues of confidentiality under *RPC* 1.6.

The obligation to preserve client confidences extends beyond merely prohibiting an attorney from himself making disclosure of confidential information without client consent (except under such

circumstances described in *RPC* 1.6). It also requires that the attorney take reasonable affirmative steps to guard against the risk of inadvertent disclosure. Thus, in Opinion 692, we stated that even when a closed client file is destroyed (as permitted after seven years), "[s]imply placing the files in the trash would not suffice. Appropriate steps must be taken to ensure that confidential and privileged information remains protected and not available to third parties." 163 *N.J.L.J.* 220, 221 (January 15, 2001) and 10 *N.J.L* 154 (January 22, 2001). Similarly, in ACPE Opinion 694 and CAA Opinion 28 (joint opinion), we joined with the Committee on Attorney Advertising in finding that two separate firms could not maintain shared facilities where "the pervasive sharing of facilities by the two separate firms as described in the Agreement gives rise to a serious risk of a breach of confidentiality that their respective clients are entitled to." 174 *N.J.L.J*. 460 and 12 *N.J.L*. 2134 (November 3, 2003).

And in Opinion 515, we permitted two firms to share word processing and computer facilities without becoming "office associates" within the meaning of *R.* 1:15-5(b), but only after noting that "the material relating to individual cases of each attorney is maintained on separate 'data' disks used only by their respective secretaries and stored (while not in use) in each of their separate offices." 111 *N.J.L.J*. 392 (April 14, 1983).

> We stress that whenever attorneys enter into arrangement as outlined herein, the attorneys must exercise reasonable care to prevent the attorney's employees and associates, as well as others whose services are utilized by the attorney, from disclosing or using confidences or secrets of a client.
>
> The attorneys should be particularly sensitive to this requirement and establish office procedures that will assure that confidences or secrets are maintained.

Id.

The critical requirement under *RPC* 1.6, therefore, is that the attorney "exercise reasonable care" against the possibility of unauthorized access to client information. A lawyer is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access. "Reasonable care," however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all

unauthorized access. Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file room, or that someone will not illegally intercept his mail or steal a fax.

What the term "reasonable care" means in a particular context is not capable of sweeping characterizations or broad pronouncements. But it certainly may be informed by the technology reasonably available at the time to secure data against unintentional disclosure. Obviously, in this area, changes in technology occur at a rapid pace. In 1983, for instance, when Opinion 515 was published, the personal computer was still somewhat of a novelty, and the individual floppy disk was the prevailing data storage device. The "state of the art" in maintaining electronic security was not very developed, but the ability to prevent unauthorized access by physically securing the floppy disk itself satisfied us that confidentiality could be maintained. By implication, at the time we were less accepting of data stored on a shared hard drive, even one that was partitioned to provide for individual private space for use by different firms, because of the risk of breach of confidentiality under prevailing technology.

We are of course aware that floppy disks have now become obsolete, and that it is exceedingly unlikely in this day and age that different law firms would attempt to share hard drive space on a conventional desktop computer, given the small cost of such computers in today's market. New scenarios have arisen, however. It is very possible that a firm might seek to store client sensitive data on a larger file server or a web server provided by an outside Internet Service Provider (and shared with other clients of the ISP) in order to make such information available to clients, where access to that server may not be exclusively controlled by the firm's own personnel. And in the context originally raised by the inquirer, it is almost always the case that a law firm will not have its own exclusive email network that reaches beyond its offices, and thus a document sent by email will very likely pass through an email provider that is not under the control of the attorney.

We are reluctant to render an specific interpretation of *RPC* 1.6 or impose a requirement that is tied to a specific understanding of technology that may very well be obsolete tomorrow. Thus, for instance, we do not read *RPC* 1.6 or Opinion 515 as imposing a per se requirement that, where data is available on a secure web server, the server must be subject to the exclusive command and control of the firm through its own employees, a rule that would categorically forbid use of an outside ISP. The very nature of the Internet makes the location of the physical equipment somewhat irrelevant, since it can be accessed remotely from any other Internet address. Such a requirement would work to the disadvantage of smaller firms for which such a dedicated IT staff is not practical, and deprive them and their clients of the potential advantages in enhanced communication as a result.

Moreover, it is not necessarily the case that safeguards against unauthorized disclosure are inherently stronger when a law firm uses its own staff to maintain a server. Providing security on the Internet against hacking and other forms of unauthorized use has become a specialized and complex facet of the industry, and it is certainly possible that an independent ISP may more efficiently and effectively implement such security precautions.

We do think, however, that when client confidential information is entrusted in unprotected form, even temporarily, to someone outside the firm, it must be under a circumstance in which the outside party is aware of the lawyer's obligation of confidentiality, and is itself obligated, whether by contract, professional standards, or otherwise, to assist in preserving it. Lawyers typically use messengers, delivery services, document warehouses, or other outside vendors, in which physical custody of client sensitive documents is entrusted to them even though they are not employed by the firm. The touchstone in using "reasonable care" against unauthorized disclosure is that: (1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data. If the lawyer has

come to the prudent professional judgment he has satisfied both these criteria, then "reasonable care" will have been exercised.[1]

[1] In the specific context presented by the inquirer, where a document is transmitted to him by email over the Internet, the lawyer should password a confidential document (as is now possible in all common electronic formats, including PDF), since it is not possible to secure the Internet itself against third party access.