Lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely. The lawyer should research the service provider to be used.

Note: This opinion was affirmed by the Board of Governors with slight modification on July 26, 2013.

RPC: 4-1.6

The Professional Ethics Committee has been directed by The Florida Bar Board of Governors to issue an opinion regarding lawyers’ use of cloud computing. “Cloud computing” is defined as "Internet-based computing in which large groups of remote servers are networked so as to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources." It is also defined as "A model of computer use in which services stored on the internet are provided to users on a temporary basis." Because cloud computing involves the use of a third party as a provider of services and involves the storage and use of data at a remote location that is also used by others outside an individual law firm, the use of cloud computing raises ethics concerns of confidentiality, competence, and proper supervision of nonlawyers.

In other words, cloud computing involves use of an outside service provider which provides computing software and data storage from a remote location that the lawyer accesses over the Internet via a web browser, such as Internet Explorer, or via an “app” on smart phones and tablets. The lawyer’s files are stored at the service provider’s remote server(s). The lawyer can thus access the lawyer’s files from any computer or smart device and can share files with others. Software is purchased, maintained, and updated by the service provider. Many lawyers and others are computing “in the cloud” because of convenience and potential cost savings.

The main concern regarding cloud computing relates to confidentiality. Lawyers have an obligation to maintain as confidential all information that relates to a client’s representation, regardless of the source. Rule 4-1.6, Rules Regulating The Florida Bar. A lawyer may not voluntarily disclose any information relating to a client’s representation without either application of an exception to the confidentiality rule or the client’s informed consent. A lawyer has the obligation to ensure that confidentiality of information is maintained by nonlawyers under the lawyer’s supervision, including nonlawyers that are third parties used by the lawyer in the provision of legal services. See, Florida Ethics Opinion 07-2 and 10-2.

Additionally, this Committee has previously opined that lawyers have an obligation to remain current not only in developments in the law, but also developments in technology that affect the practice of law. Florida Ethics Opinion 10-2. Lawyers who use cloud computing therefore have an ethical obligation to understand the technology they are using and how it potentially impacts confidentiality of information relating to client matters, so that the lawyers may take appropriate steps to comply with their ethical obligations.

Other states that have addressed the issue of cloud computing have generally determined that there are ethics concerns regarding confidentiality of information, but that a lawyer may compute via the cloud if the lawyer takes reasonable steps. See, e.g., Alabama Ethics Opinion 2010-02 (Lawyer may outsource storage of client files through cloud computing if they take reasonable steps to make sure data is protected); Arizona Ethics Opinion 09-04 (2009) (Lawyer may use online file storage and retrieval system that enables clients to access their files over the Internet, as long as the firm takes reasonable precautions to protect confidentiality of the information); Iowa Ethics Opinion 11-01 (2011) (Appropriate due diligence a lawyer should perform before storing files electronically with a third party using SaaS (cloud computing), includes determining that the lawyer will have adequate access to the stored information, the lawyer will be able to restrict access of others to the stored information, whether data is encrypted and password protected, and what will happen to the information in the event the lawyer defaults on an agreement with the third party provider or terminates the relationship with the third party provider); Nevada Formal Ethics Opinion 33 (2006) (Attorney may store client files electronically on a remote server controlled by a third party as long as the firm takes precautions to safeguard confidential information such as obtaining the third party’s agreement to maintain confidentiality); New York State Bar Ethics Opinion 842 (2010) (Lawyer may use an
online computer data storage system to store client files provided the attorney takes reasonable care to maintain confidentiality, and the lawyer
must stay informed of both technological advances that could affect confidentiality and changes in the law that could affect privilege); and
Pennsylvania Ethics Opinion 2011-200 ("An attorney may ethically allow client confidential material to be stored in 'the cloud' provided the
attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure
that the data is protected from breaches, data loss and other risks”).

This Committee agrees with the opinions issued by the states that have addressed the issue. Cloud computing is permissible as long as the
lawyer adequately addresses the potential risks associated with it. As indicated by other states that have addressed the issue, lawyers must
perform due diligence in researching the outside service provider(s) to ensure that adequate safeguards exist to protect information stored by the
service provider(s). New York State Bar Ethics Opinion 842 suggests the following steps involve the appropriate due diligence:

- Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will
  notify the lawyer if served with process requiring the production of client information;
- Investigating the online data storage provider’s security measures, policies, recoverability methods, and other procedures to determine if they
  are adequate under the circumstances;
- Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.

Of particular practical assistance is Iowa Ethics Opinion 11-01. As suggested by the Iowa opinion, lawyers must be able to access the lawyer’s
own information without limit, others should not be able to access the information, but lawyers must be able to provide limited access to third
parties to specific information, yet must be able to restrict their access to only that information. Iowa Ethics Opinion 11-01 also recommends
considering the reputation of the service provider to be used, its location, its user agreement and whether it chooses the law or forum in which
any dispute will be decided, whether it limits the service provider’s liability, whether the service provider retains the information in the event the
lawyer terminates the relationship with the service provider, what access the lawyer has to the data on termination of the relationship with the
service provider, and whether the agreement creates “any proprietary or user rights” over the data the lawyer stores with the service provider. It
also suggests that the lawyer determine whether the information is password protected, whether the information is encrypted, and whether the
lawyer will have the ability to further encrypt the information if additional security measures are required because of the special nature of a
particular matter or piece of information. It further suggests that the lawyer consider whether the information stored via cloud computing is also
stored elsewhere by the lawyer in the event the lawyer cannot access the information via “the cloud.”

This Committee agrees with the advice given by both Iowa and New York State. Additionally, this Committee believes that the lawyer should
consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has
proprietary client information or has other particularly sensitive information.

In summary, lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is
maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely.
The lawyer should research the service provider to be used.

http://dictionary.reference.com/browse/cloud%20computing>

2 Id.

[Revised: 07-30-2013]