L.E.O. 2012-01

USE OF ELECTRONIC MEDIA FOR FILE STORAGE

INTRODUCTION

The Lawyer Disciplinary Board sees the need to issue a formal advisory opinion on electronic storage. This is based on a question we received about retention and destruction of closed client files kept in electronic form and our belief that we needed a formal opinion to address broader issues.

Rule 1.6(a)of the West Virginia Rules of Professional Conduct provides that "[a] lawyer shall not reveal information relating to representation of a client unless the client consents after consultation." The attorney's use of electronic storage is permissible under the West Virginia Rules of Professional Conduct, but there must be a protection of the client's confidences. The Lawyer Disciplinary Board previously addressed the retention and destruction of closed client files in L.E.I. 2002-01. This opinion is to be used in conjunction with that opinion in regards to electronic storage. The attorney should always remember that the client file belongs to the client. *See* L.E.I 89-02, 92-02, and 02-01. The primary concern regarding file retention is the accessibility by the client to his property. This L.E.O. is intended to address only obligations under the West Virginia Rules of Professional Conduct, but lawyers are reminded that information in their files may also contain other protected information such as social security numbers, health information, etc., which this L.E.O. does

not specifically address, but which the lawyer may have liability or responsibility for disclosure under federal or state law.

The West Virginia Rules of Professional Conduct do not limit the way in which the client file is retained. While explicit consent is not required, the attorney may want to advise of the method of file storage and destruction in the retainer agreement or engagement letter. The attorney can use the various sources of electronic storage that are available, but certain precautions should be taken to ensure the attorney has used due diligence to protect the client's file, client's confidentiality, accessibility, and file integrity as follows[1]:

CONFIDENTIALITY - due diligence requires consideration of:

- Security of data
  (e.g. during transmission to off-site storage, during storage and during destruction of file)

- Control of the data by the attorney
  (e.g. Who has access to stored data? What happens if lawyer cannot pay storage bill? What country is the data stored in, and how might that country's laws affect privacy/ownership of the data? If provider sells company, what changes might occur to data or the contract to store data?)

- Safeguarding of privilege
  (e.g. monitoring emerging law regarding online storage and waiver/loss of privilege)

---

[1] These same issues have been reviewed by other jurisdictions and a review of those opinions can be helpful. For example, the Penn. Bar Ass'n Comm. on Legal Ethics and Professional Responsibility, Formal Op. 2011-200 (2011) describes potential pitfalls for practice as technology rapidly advances, and provides helpful discussion of what might be included in a standard of reasonable care for protecting client and attorney interests. As always, attorneys should note that what may be allowable in one jurisdiction may not be allowable in West Virginia.

- State and federal laws that apply to retention and destruction of documents containing personally identifiable information
  (e.g. HIPAA)

ACCESSIBILITY - due diligence requires consideration of:

- Maintenance of compatible technology for access/reproduction throughout the duration of the file's retention (may want to disclose electronic storage to clients in retainer agreement or engagement letter; can client reproduce the file from electronic format?)

- Alternative access when lawyer no longer available
  (e.g. Who would have passwords? Authorization on accounts? Who could access files of practitioners who abandon their practice or pass away?)

FILE INTEGRITY - due diligence requires consideration of:

- Retention of originals where legally necessary

- Inclusion of relevant communications that may be considered part of the client file
  (e.g. emails, electronically filed documents, voice mail communications, etc.)

- Prevention of inadvertent destruction/modification/degradation of data
  (e.g. quality)

- Backup of all data

CONCLUSION

While the Board finds use of electronic storage of client files to be permissible under the Rules of Professional Conduct, the attorney must ensure not only the confidentiality of

the data and its accessibility to the client, but also the integrity of the file. The use of an electronic storage provider presents additional issues that should be considered.

APPROVED by the Lawyer Disciplinary Board on the 14th day of September, 2012, and **ENTERED** this 14 day of September, 2012.

Charles J. Kaiser, Jr., Chairperson
Lawyer Disciplinary Board