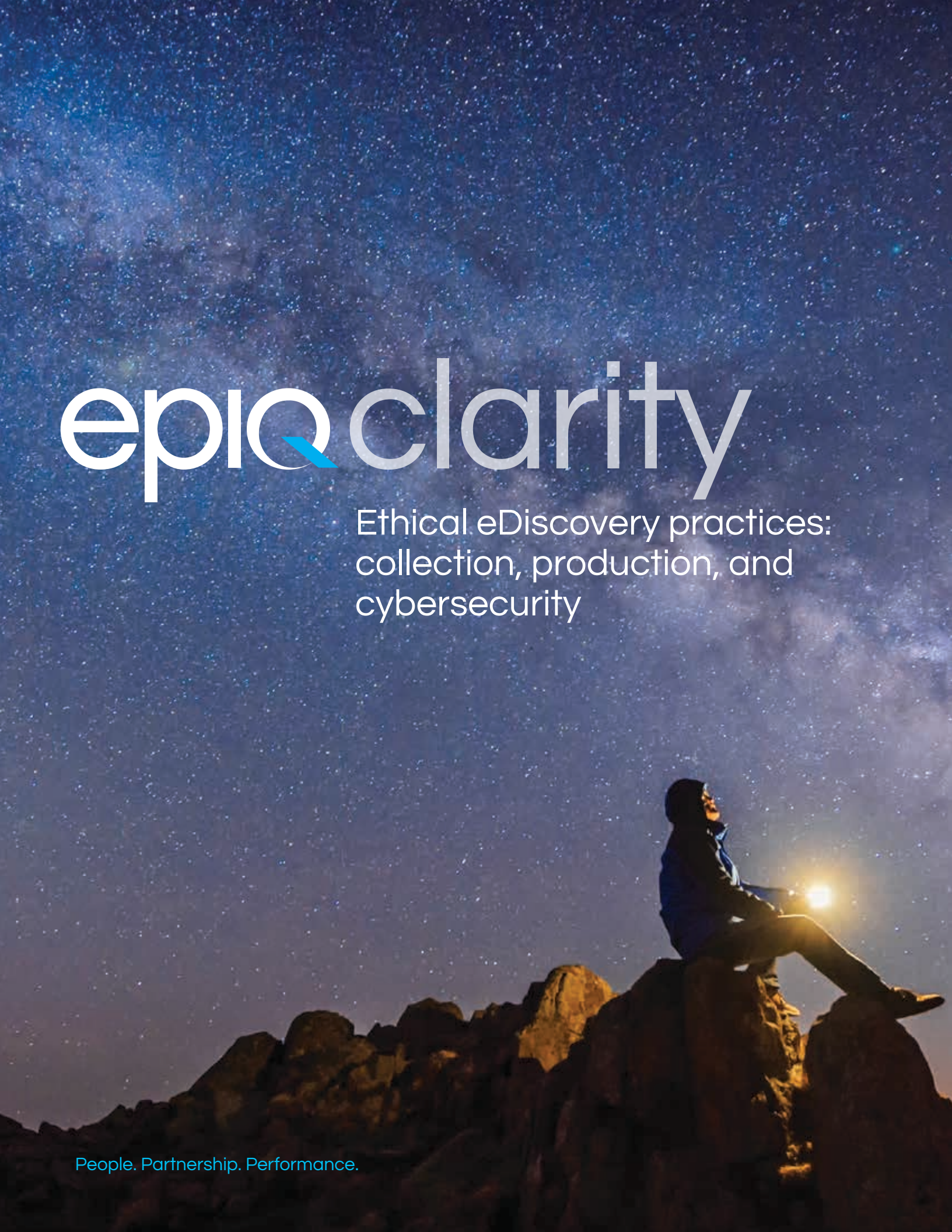
epiq clarity
Ethical eDiscovery practices: collection, production, and cybersecurity
People. Partnership. Performance.

Introduction

In today's legal practice, almost all litigators regularly deal with eDiscovery. The overwhelming majority of lawyers and their clients store data and communicate electronically. Because of this, the amount of data that lawyers will eventually need to retrieve and produce during litigation is more than ever before. Many lawyers also utilize technology solutions as a litigation aid, which carries many advantages. This includes cutting down on costs, improving the quality of discovery production, and faster case resolution. While these benefits are great, lawyers who encounter eDiscovery and electronically stored information (ESI) must familiarize themselves with the relevant ethical rules. Several of the American Bar Association (ABA) Model Rules of Professional Conduct apply to situations involving data preservation, collection, review, production, and security.[1]

Preservation and collection practices

In general

Lawyers have ethical duties to preserve and disclose all information that is relevant to a lawsuit. Under ABA Model Rule 3.4(a), lawyers are prohibited from unlawfully obstructing another party's access to evidence or unlawfully altering, destroying, or concealing a document with potential evidentiary value. Additionally, ABA Model Rule 3.3 requires that lawyers act with candor towards the court. As such, during discovery lawyers must disclose all relevant documents (other than those protected by privilege) in their original format to avoid violating these rules.

The first step should always be preservation. The failure to preserve relevant data can result in spoliation of evidence claims and significant sanctions. Because of this, lawyers and their clients should execute sound preservation practices even before litigation ensues. At the outset of representation, lawyers should advise their clients on best practices to ensure they do not lose important data. This includes the following:

1. **Monitor the way employees communicate and transmit business data.** An organization should be aware of what technology their employees use to create and share information both internally and externally. Since technology and communication trends are rapidly changing, organizations must investigate these practices on a regular basis in order to accurately evaluate the best way to preserve business data.
2. **Create policies and provide training about acceptable ways to handle business data and preservation practices.** Doing this makes employees aware of acceptable technology usage and ways to securely preserve important documents. To avoid data loss and future legal issues, key documents must be backed up or securely saved.

Implementing these practices before litigation will help prevent future roadblocks. Generally, organizations must take reasonable efforts to preserve relevant data when litigation is reasonably anticipated, threatened, or pending.[2] After a lawsuit is filed, it is good practice for lawyers to immediately issue a litigation hold. This will outline categories of information that could be relevant to the lawsuit and a request to the client to preserve this data so it can be reviewed and potentially disclosed in discovery. At the outset, the scope of the litigation hold will be broader because many facts relevant to the claim are unknown. As the lawsuit progresses, the litigation hold should be amended and narrowed if appropriate.

Lawyers will then need to work with their client to identify and collect any ESI that is relevant

[1] The majority of states have adapted identical or similar ethics rules.
[2] 11 Sedona Conf. J. 267 (2010)

to the lawsuit. This task can be daunting when dealing with a large amount of potentially relevant ESI located in several places. Determining what information clients need to preserve and the appropriate data custodians are important steps.[3] Lawyers should interview the custodians to understand where essential information is located and what processes are being utilized to ensure preservation. Following these steps will help lawyers fulfill their ethical obligations when it comes time to review and disclose documents with evidentiary value during discovery.

Social media considerations

Lawyers must also implement ethical social media collection practices. For example, counsel cannot friend request a party, witness, or juror on a social media website in order to gain access to their private information for purposes of collecting data to use in litigation. This could potentially violate several ABA rules, including Rule 4.2 (communication with represented person), Rule 4.3 (communication with unrepresented person), and Rule 8.4(c) (conduct involving dishonesty, fraud, deceit or misrepresentation).[4] It is also unethical to advise clients to friend request someone for this purpose. However, data that is publicly available for viewing is fair game. Another obstacle with social media collection is that users can easily delete or change their content. As such, lawyers may need to send a subpoena to the actual social media provider in order to obtain relevant information.[5]

Employing adequate social media collection practices is necessary to avoid any ethical violations. For example, merely taking a screenshot or printing out a social media webpage may not be an accurate reflection of the content because it may not include certain metadata, videos, or other embedded information.[6] This could be a potential Rule 3.4 violation if the missing data holds evidentiary value. For social media data containing relevant evidence, lawyers must provide proper authentication and include all key data in the production. More technically involved collection methods include dynamic capture and content downloading from the provider.[7]

Rule 3.4 also applies to situations where a lawyer advises a client to delete or alter social media content that is relevant to a lawsuit. The Sedona Conference recently weighed in on this issue:

> Several states have issued ethics opinions or guidelines relating to attorneys counseling clients regarding their use of social media. Those opinions generally provide that attorneys may advise clients regarding changing privacy settings or removing content, as long as they also satisfy preservation ob-ligations and do not obstruct another party's access to evidence. In other words, "unless an appropriate record of the social media content is preserved, a party or nonparty may not delete information from a social media account that is subject to a duty to preserve." For example, an attorney may advise a client regarding changing privacy or security settings to limit access to the client's social media outside of the formal discovery context. Similarly, an attorney may advise a client to "take down" or remove content, as long as it is does not violate substantive law or the duty to preserve.[8]

As such, lawyers must be careful when instructing clients about their past and future social media

[3] 11 Sedona Conf. J. 277 (2010)
[4] The Sedona Conference Primer on Social Media, Second Edition, pp. 49-50 (July 2018 Public Comment Version)
[5] Id at 19.
[6] Id at 22-23.
[7] Id at 23-26.
[8] Id at 47-48.

activity. Failure to preserve significant evidence can result in sanctions, license suspension, and an unfavorable litigation outcome.

Review and production of eDiscovery

Lawyers must also understand their ethical duties when it comes time to review and produce discovery. The duties of competence and confidentiality are crucial at this stage of litigation. ABA Model Rule 1.1 requires lawyers to provide competent representation to their clients. As of 2012, this includes keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. While lawyers obviously do not need to be information technology experts, they must understand the basic features of technology commonly used in legal practice.[9] This rule comes into play when evaluating eDiscovery review solutions, which many lawyers use to quickly and efficiently review larger data sets. If a specific program has a breach history or otherwise appears to be a risky investment, lawyers should explore alternatives.

Lawyers use many different type of technology to review and produce discovery, such as email, cloud, and eDiscovery review software. While this is standard practice and very beneficial, lawyers must keep their clients confidential and privileged information safe. ABA Model Rule 1.6 requires lawyers to keep client information confidential unless the client provides informed consent.[10] Section (c) to this rule states: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." This section was created to address the security risks that new technology poses. Comment 18 explains that lawyers must safeguard sensitive client data against unauthorized access by third-parties and unauthorized or inadvertent disclosure by both the lawyer and individuals they supervise who also handle this data. However, this obligation will still be met as long as the lawyer makes reasonable efforts[11] to prevent access or disclosure to the information, even if the data gets hacked. In order to fulfill this obligation, lawyers must research and compare different technology before storing client information on them. Some key factors to evaluate include accessibility, encryption, prior breach history, and reputation. Lawyers who use third-party platforms must also supervise their security measures to some degree in order to ensure confidentiality.

Even after taking appropriate steps to protect confidentiality, lawyers may encounter a situation where they inadvertently produce privileged information. Another way lawyers who litigate in federal court can protect their clients' privilege and satisfy Rule 1.6 is to obtain a Rule 502(d) order. This will require opposing counsel to return any mistakenly disclosed documents that contain privileged information without waiver.

Data privacy

As noted in the previous section, protecting confidential client data must always be a top priority for legal professionals during every phase of litigation. Storing and sharing data electronically unfortunately increases the risk

9 ABA Formal Opinion 477R* (May 11, 2017; Revised May 22, 2017)

10 Other exceptions are if disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted. ABA Model Rule 1.6(a), Confidentiality of Information.

11 Factors to consider in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). Rule 1.6, Comment 18

for a security breach. Law firms must ensure that their internal infrastructure is adequately protected. In addition, before entering into a business relationship with a third-party vendor or purchasing eDiscovery review software, firms must research the security measures that the outside organization employs. Researching the benefits and risks of current technology helps lawyers choose a secure program they can use without fear of compromising confidential client data, helping to fulfill their ethical obligations of competence and confidentiality. Another good practice is avoiding the use of unsecured public networks. If lawyers have to conduct business on public Wi-Fi, they should use a cloud-based solution or secure their devices. Additionally, firms should hire information technology specialists or consult with external technology experts when determining how to secure their networks and devices.

Protecting client data can seem like a overwhelming task in today's ever-changing technological world. The ABA recently addressed the issue of confidentiality and technology, concluding that lawyers must take reasonable measures to prevent inadvertent disclosure of confidential and privileged information. The level of security required will depend on the sensitivity of the information. For example, lawyers are often exposed to a client's trade secrets or financials during discovery review. Sometimes this information is relevant to the lawsuit and will require disclosure. In this case, a lawyer must ensure they handle this data with the utmost care during litigation. If the data is irrelevant, lawyers must take the same measures to prevent inadvertent disclosure. Since this sensitive data will likely be stored on the firm's network, it is also vulnerable to hacking. In the unfortunate event that a breach occurs, even after taking appropriate steps to protect sensitive client data, lawyers "have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation."[12]

[12] ABA Formal Opinion 483 (October 17, 2018)

Conclusion

Just as with virtually every other field of business, using technology is a staple in the legal practice. While using technology to conduct business is highly beneficial, it also heightens a lawyer's ongoing ethical obligations. During litigation, lawyers must use sound practices when preserving, collecting, reviewing, producing, and safeguarding ESI. Lawyers must stay on top of emerging technology and evaluate the risks before using it in practice. Lawyers must also monitor work done by non-lawyers (such as law clerks and paralegals) that they retain, employ, or associate with in the course of business. Making sure that non-lawyers act in a manner compatible with the professional obligations of the lawyer is an added layer of ethical obligation.[13] Firms should provide training to their lawyers and support staff about eDiscovery ethical issues, acceptable technology use, and how to ethically integrate technology into legal practice. Periodically reviewing and updating security measures is also an extremely important practice habit. While many jurisdictions adapt to the ABA's rules, some jurisdictions depart on certain issues or have published varied opinions. To stay on top of their ethical obligations, lawyers should become familiar with the rules and opinions of each jurisdiction in which they are licensed to practice law.

---

[13] ABA Model Rule 5.3, Responsibilities Regarding Nonlawyer Assistance