Safeguarding Client Property and Information

Legal, Ethical, and Practical Imperatives

BY BRAD KANTER

Protecting client property and information is essential for legal, forensic, and behavioral professionals. Regardless of whether the process is collaborative or litigated, confidentiality, privilege, and institutional safeguards are crucial to maintaining compliance and trust. In legal, forensic, and behavioral investigative contexts, safeguarding client property and information is not merely a best practice, it is a professional, ethical, and often legal obligation. Whether handling sensitive documents, digital data, or physical assets, professionals must ensure confidentiality, integrity, and accessibility.

This article reviews the ethical, legal, and procedural standards with practical suggestions for safeguarding assets with multifaceted responsibilities involved in protecting client property and information, with particular attention to divorce proceedings, forensic investigations, and legal compliance. The required standards can be challenging to meet, and yet formal oversight is difficult to build into the process. The system relies on professionals to independently police their own actions which may result in different degrees of adherence and creating avoidable liability.

Also provided is a concrete option to ensure forensic reports and other independent service providers' results, facts, and circumstances remain privileged. In addition, this article will provide a technology option that enforces the rules and requirements of the American Bar Association (ABA) Model Rule of Professional Conduct (Model Rule) 1.6 by integrating technology into the internal control system limiting liability and creating improved adherence to safeguarding client property and information.

Ethical, Legal, and Procedural Guidance

Professionals rely on specific ethical, legal, and procedural standards to guide their actions when safeguarding client property and information. These frameworks help ensure that physical and digital assets are managed with integrity and confidentiality. Here are detailed examples illustrating how these standards are applied in practice:

- *Legal professionals:* Attorneys follow the Model Rules, such as Rule 1.6, which mandates strict confidentiality of client information. For example, a lawyer handling a divorce case must ensure that sensitive financial records are stored in secure, access-controlled digital systems and are only shared with authorized parties. When physical evidence or property is involved, lawyers may use locked storage and keep detailed logs of access and transfers.
- *Forensic accountants:* Forensic Certified Public Accountants comply with Standards for Forensic Services No. 1 (SSFS 1), which requires maintaining the integrity and confidentiality of financial data during investigations. For instance, a forensic accountant analyzing marital assets in a divorce proceeding will use encrypted software and password-protected files for client data and will avoid discussing case details in public or with unauthorized individuals.

Andriy Onufriyenko/Moment/Getty Images Plus

- *Behavioral professionals:* Psychologists and counselors must adhere to HIPAA regulations to protect personal health information. In practice, this means storing client records in locked cabinets or secure electronic health record systems and only releasing information with explicit client consent or as required by law.
- *Procedural safeguards in divorce proceedings:* When professionals are asked to temporarily hold or manage disputed assets—such as real estate deeds or joint bank accounts, they may use a neutral third-party escrow service. This ensures transparency and protects against unauthorized access or claims. Regular inventory and documentation of assets are maintained, and all parties are kept informed of asset status.
- *Technology integration:* Firms may adopt internal control systems that automate compliance with ethical rules. For example, document management platforms can restrict access based on user roles, log all activities, and encrypt sensitive files, thus enforcing confidentiality and limiting liability.

These examples demonstrate the practical steps professionals may take to uphold ethical, legal, and procedural standards for safeguarding client property and information, whether dealing with physical documents, digital data, or tangible assets.

Professional Imperatives for Safeguarding Client Property and Information

The protection of client property and information is a fundamental responsibility for professionals working in legal, forensic, and behavioral fields. Whether the process at hand is collaborative or involves litigation, the principles of confidentiality, privilege, and institutional safeguards remain central to upholding compliance and fostering trust between professionals and clients.

In investigative environments spanning legal, forensic, and behavioral domains, the act of safeguarding client property and information transcends recommended practices; it constitutes a professional, ethical, and frequently legal obligation. Professionals engaged in these contexts must manage a variety of sensitive materials, including documents, digital records, and physical assets, and are required to maintain their confidentiality, integrity, and accessibility at all times.

Contextual Application in Divorce Proceedings

While the principles of safeguarding client property and information apply broadly, their relevance is particularly acute in family law matters. The process of divorce using collaborative or litigation, and the safeguarding requirements may shift accordingly. In either scenario, the involvement of various professional services, such as financial forensics, becomes another variable that requires maintaining asset integrity and confidentiality.

For example, in a collaborative divorce, both parties may agree to work together with a financial forensic expert to value and divide marital assets. In this setting, professionals typically establish secure data-sharing platforms that allow authorized parties to review financial records while restricting access for others, ensuring confidentiality. All communications and document exchanges are logged for transparency.

In contrast, adversarial divorce litigation often involves disputes over asset ownership or allegations of hidden property. Here, attorneys and forensic accountants may use encrypted digital storage for sensitive financial documents and implement strict chain-of-custody protocols for any physical evidence, such as original deeds or account statements. Access is limited to essential personnel, and detailed logs are kept to document when and by whom records are viewed or transferred.

Additionally, when a forensic accountant is engaged to trace assets or evaluate income streams, they may utilize password-protected files and secure email channels to communicate findings with legal counsel. If a court orders a professional to hold disputed assets—such as real estate titles or joint bank funds—a neutral escrow service might be used, and regular inventories and status updates are provided to all involved parties.

Financial forensics play a crucial role in divorce matters, working closely with the litigation process to ensure that assets are properly managed and protected. The integrity of the safeguarding process in these cases depends on strict attention to confidentiality, privilege, and institutional safeguards, which together support compliance and foster trust among all parties involved. Employing various software systems to maintain the level of integrity required by our respective regulatory bodies and professional associations is essential. Those requirements incorporate the legal professions safeguarding requirements.

Confidentiality in Forensic Investigations

All financial related experts and analysts, Master Analyst Financial Forensics (MAFF-NACVA), Certified in Financial Forensics (CFF – AICPA) Certified Forensic Examiners (CFE-ACFE), Certified forensic interviewers (CFI-IAI), CPA (AICPA) and behavioral analysts must obtain informed consent, anonymize data, and use secure storage and transmission methods. Forensic reports may be protected under attorney-client privilege or the work-product doctrine.

However, courts increasingly scrutinize these claims, as seen in cases like *In re: Capital One Customer Data Security Breach Litigation* (2020) and *Leonard v. McMenamins*. Understanding how to formalize and clarify the attorney client privilege relationship should not be left for interpretation or an unwanted surprise of an interpretation you did not anticipate. Our responsibilities as the professional "in charge"

of the matter demands a proactive and systemic methodology built into your work protocols.

One such method to ensure confidentiality and maintaining attorney client privileged protection is the use of a Kovel letter.

Kovel Letter

A Kovel letter is a formal legal document that extends attorney-client privilege to third-party experts, such as accountants, financial analysts, or consultants, who are retained by an attorney to assist in providing legal advice.

This concept stems from the 1961 case United States v. Kovel, which established the Kovel doctrine and clarified that the expert is engaged by the attorney, not directly by the client, with the expert's work intended to support the attorney's legal counsel. The privilege applies only if the expert acts as an agent of the attorney, the expert's input is essential for the attorney's legal advice, and all communications remain confidential and undisclosed to third parties.

The court in *U.S. v. Kovel* likened the expert's role to that of a translator, helping the attorney understand complex subjects such as financial data. To ensure the privilege is preserved, the engagement letter must explicitly state that the expert operates under the attorney's direction, avoids acting independently or providing services outside the scope of legal advice, and maintains confidential communications within the attorney-client-expert relationship.

However, if the expert provides business advice rather than legal assistance, is retained directly by the client, or if communications are improperly documented or disclosed to outsiders, courts may rule that privilege does not apply, and it can be waived.

Organizations must educate staff, establish clear procedures, and conduct audits. In case of a breach, professionals must contain the incident, notify stakeholders, and investigate the cause. The ABA recommends having a formal incident response plan.

Emerging Challenges and Future Considerations

Professionals must stay current with evolving threats, use secure platforms, and monitor third-party vendors. Recent cases show courts narrowing the scope of privilege. Documentation of intent and limited distribution are key to preserving protection. It should be of no surprise to us all that technology provides enhanced efficiency, convenience and productive resources. It is also not surprising that technology has and will be used to steal and compromise electronic data, putting you and your clients at risk. Your risk as a lawyer goes beyond the monetary as you are held to account to safeguard your client's information.

Cyber Liability Insurance for Law Firms

It is recommended that your professional liability insurance have cyber-attack insurance to financially and legally insulate you and your firm's exposure. Lawyer liability insurance for cyber-attacks, called cyber liability insurance is designed to protect law firms and attorneys from the financial and legal consequences of cyber incidents. These incidents include data breaches, ransomware, phishing, wire fraud, and other forms of cybercrime that target sensitive client information and firm operations.

Law firms are prime targets for cybercriminals due to the volume of confidential data they hold—client financials, health records, trade secrets, and privileged communications. Even small firms are vulnerable, and a single breach can result in:

- Financial loss
- Reputational damage
- Regulatory penalties
- Loss of client trust

Recent surveys show that up to 42% of large law firms have experienced a data breach, and the American Bar Association (ABA) now considers cyber risk management a core ethical duty for attorneys.

Cyber liability insurance typically provides coverage for several key risks that law firms face in today's digital environment. It includes data breach response costs, such as notifying affected clients, offering credit monitoring, and managing public relations after an incident. This insurance also covers expenses related to ransomware or extortion, including payments to hackers and restoring compromised systems. Business interruption losses, resulting from downtime due to cyber incidents, are generally covered as well. Additionally, policies often pay regulatory fines imposed for noncompliance with privacy laws such as HIPAA and GDPR. Legal defense costs for lawsuits brought by affected clients are included, as are losses stemming from social engineering and wire fraud, such as fraudulent fund transfers. This comprehensive protection helps law firms mitigate the financial and reputational impact of cyber threats.

Law firms should follow several best practices to reduce their exposure to cyber risks and ensure adequate insurance protection. First, it is important to assess the firm's risk profile by evaluating the amount and sensitivity of the data stored and considering the potential costs of a breach. Firms should also review client agreements and contractual obligations, as some clients may require law firms to maintain specific cyber insurance limits. Strengthening cybersecurity controls is essential, as insurers may offer better rates and higher coverage limits to firms that demonstrate robust security measures. Lastly, firms must understand policy exclusions, since cyber insurance typically does not cover property damage or the loss of intellectual property.

The Model Rules, specifically Rules 1.1, 1.6, and 1.15, mandate that attorneys must protect client property and

ActivTrak Benefits in Family Law Divorce Cases

Benefit	Description	Relevance to Divorce Cases
Privacy-First Data Protection	Default privacy settings, data hashing, no intrusive collection	Protects sensitive client data
Granular Access Controls	Role-based permissions, custom groups, Do Not Track lists	Limits access to authorized personnel
Data Security & Compliance	Encryption, audit logs, alarms, regulatory support	Ensures legal and ethical compliance
Transparent Monitoring	Productivity insights without invasive surveillance	Balances oversight with privacy
Incident Response	Logs and alarms for breach containment and investigation	Rapid response to data incidents

information, which include safeguarding digital assets. Neglecting these duties can expose attorneys to significant consequences such as sanctions, loss of their professional license, or even civil liability. In today's digital landscape, carrying cyber insurance is widely recognized as a best practice to help attorneys fulfill these legal and ethical obligations.

Lawyer liability insurance for cyber-attacks is now a critical component of risk management for law firms. It protects against the financial, legal, and reputational fallout of cyber incidents, and is increasingly required by clients and regulators. The best approach is to assess your firm's risk, strengthen your cybersecurity posture, and select coverage that fits your needs.

Monitoring and Tracking Software in Family Law Matters

Monitoring software can play a critical role in family divorce cases due to the highly sensitive nature of client data, such as financial records, health information, custody documents, and privileged communications.

Legal and ethical obligations require attorneys, forensic accountants, and other professionals to protect this information from unauthorized access and breaches. Solutions like ActivTrak offer several benefits for safeguarding client data as they are built with privacy as a foundational principle, avoiding intrusive data collection and applying cryptographic hashing to sensitive information, which is particularly vital in legal contexts where confidentiality is crucial. ActivTrak also enables granular, role-based access controls, allowing only authorized personnel to view sensitive client details and supporting strict confidentiality through custom groups and "Do Not Track" lists.

The platform ensures data security and compliance with regulations such as GDPR, CCPA, and HIPAA by using end-to-end encryption and maintaining SOC 2 Type 1 & 2 certifications. Audit logs and security alarms help investigate data access or changes and facilitate rapid incident response, supporting legal teams in upholding chain-of-custody protocols and responding efficiently to breaches in line with ABA recommendations.

While certain advanced features like screenshots are available as add-ons and require careful use to avoid privacy concerns, and customization for specific workflows may be limited, ActivTrak's strengths can be enhanced by combining it with other security measures, including encryption, secure backups, multi-factor authentication, and regular audits. Additionally, consistent staff training on confidentiality protocols and diligent record-keeping of file access and modifications using ActivTrak's audit features are essential best practices for law firms handling divorce cases.

Software like ActivTrak offers robust privacy, security, and monitoring features that help law firms safeguard client information and digital data in family law divorce cases. Its privacy-first approach, granular access controls, and compliance support make it a valuable tool for protecting sensitive assets and maintaining trust in high-stakes legal environments.

Conclusion

Safeguarding client property and information is a cornerstone of ethical and legal practice in law, forensic investigation, and behavioral analysis. From managing assets during divorce to protecting digital data and responding to subpoenas, professionals must implement robust safeguards and remain vigilant. As threats evolve and legal standards shift, ongoing education, clear policies, and proactive strategies are essential to uphold trust, integrity, and compliance while minimizing legal liability. FA

BRAD KANTER, CPA/CGMA/CFF, CFE, CFI, CVA/MAFF, EA, FCPA, MAC is the principal of Kanter Financial Forensics and Kanter Consulting Group, leading with deep expertise in financial forensics—including business valuations, fraud detection and examination, tax analysis, economic damages, complex financial analysis, and credibility analysis.