Calloquy

The Next Era of Litigation

Securing Remote Litigation

Why a new era of legal proceedings requires new levels of security

Securing Remote Litigation

The next era of litigation is here. It requires accessibility, accuracy, and reliability. It requires a remote litigation platform that allows remote and distributed litigation teams to function with as much ease, as much confidence, and as much assurance that their communications are safe, as if they were in that client meeting, deposition, mediation, or arbitration in person.

That is exactly what Calloquy does. Calloquy is a remote litigation platform designed for litigators and encompassing all stages of litigation. Calloquy is a safer, more secure virtual environment than mass-market videoconference platforms. It must be – because as a lawyer *you* have a duty of confidentiality to your clients and, according to the ABA, that duty compels lawyers using technology to take efforts "to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information."[1]

1. American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 498 (Mar. 10, 2021), available at: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf

1. The Attorney's Duty

When it comes to keeping data secure, the duties and challenges which attorneys face are numerous and multifaceted. To be certain, the data of every industry, every company, every person's data is valuable. And while every company has a duty to their customers and shareholders, clients *entrust* attorneys with their most sensitive information – information at the center of an adversarial proceeding and information which warrants top-notch security.

According to IBM's **Cost of a Data Breach Report 2022**, the average total cost of a data breach increased from $3.86 million in 2020 to an all-time high of $4.35 million in 2022. The report signals a 10% year-over-year increase in the average total cost of a breach.

Personally identifiable information (PII) breaches now have a cost of $161 per compromised record for the breached organizations. The average number of days it took to identify a breach increased from 287 days to 316 days as the pandemic forced many into remote workforce situations.

The market demands attorneys use technology.

Technology generates more opportunities for attorneys – but it also creates more risks. Clients prefer to participate in virtual meetings from their desk or conference rooms rather than make a trip to their law firm's office. And if a client's appearance at a court proceeding is perfunctory, then they prefer to attend that remotely also. Clients prefer this because it saves them a great deal of time and a great deal of money.

Clients consider video conferencing a significant upgrade from a phone call. Clients can speak face to face and upload and review documents with their attorneys as though everyone were in the same room. Innovative law firms must implement technology which allows them to hold virtual meetings with clients across town and across the world.

Attorneys must market themselves as being faster, more accurate, better informed, more prepared, and more secure. Technology helps you be all those things - when you have the right technology. Firms that position themselves as innovators can proclaim to existing and prospective clients that their commitment to technology sets them apart from other firms.

Calloquy allows a client, an attorney, a deponent, or arbitration witness to **annotate, highlight, or otherwise draw on exhibits in real time.**

The profession demands attorneys use technology.

Those establishing the rules which govern the profession are demanding attorneys use technology. And they are demanding that attorneys use technology safely. In 2012, the ABA amended Comment 8 to the Model Rules of Professional Conduct Rule 1.1 to require lawyers to keep abreast of the technology which affects the profession. For a change-resistant profession, this was a tremendous revision.

> **" Rule 1.1: Competence:** A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation."
>
> **"Comment (8):** To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including **the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

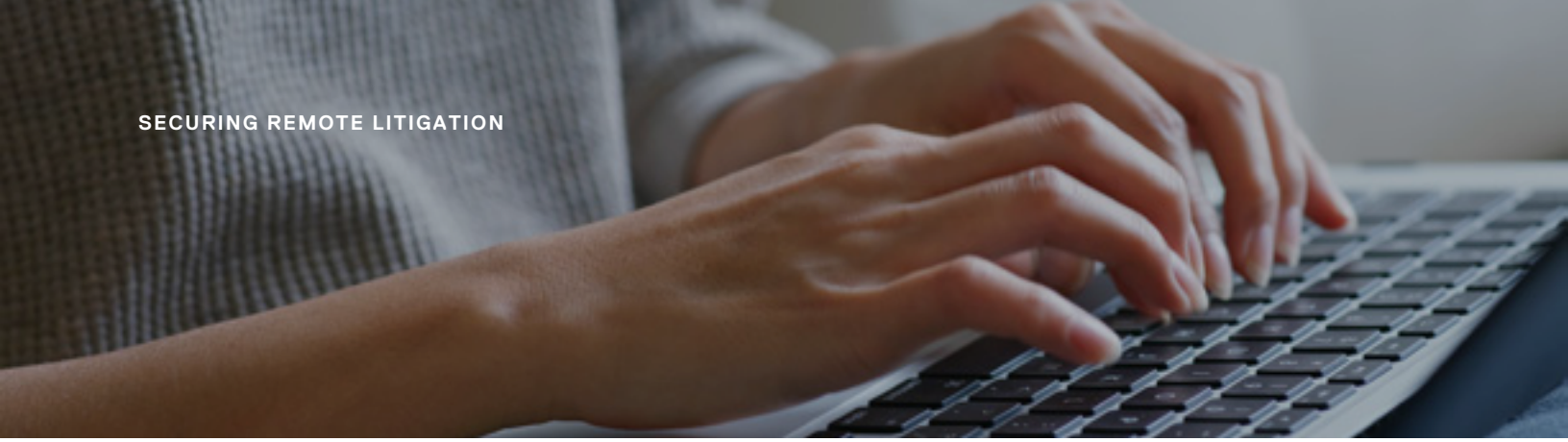
In March 2021, the ABA released Formal Opinion 481, which considered the ethical duties of lawyers practicing law in a virtual environment. In this Opinion, the ABA acknowledged that several rules are implicated by the virtual practice of law, including the duties of competence (Model Rule 1.1), diligence (Model Rule 1.3), communication (Model Rule 1.4), confidentiality (Model Rule 1.6), and the duty to supervise the work of subordinate lawyers and nonlawyers (Model Rule 1.6). "Guided by the rules," the ABA noted that a lawyer must take affirmative steps to safeguard communications, including using "secure internet access methods to communicate, access and store client information," including implementing systems that require complex passwords, encrypting data, and using multi-factor authentication.

With regard to virtual meeting platforms and document repositories, the ABA provided the following guidance:

- Access to accounts and meetings should be only through strong passwords;
- The lawyer should explore whether the platform offers higher tiers of security over video conferencing systems used by the general public;
- Recordings or transcripts should be securely stored;
- The platform should obtain consent before initiating recordings;
- Steps should be taken to ensure that privileged conversations are not accessible by others not represented by the lawyer; and
- Document repositories should be secure and sensitive information should be encrypted.

Rule 502(b) of the Federal Rules of Evidence governs the inadvertent disclosure of privileged communications, the sort of inadvertent disclosure that might come from a videoconference or chatroom hack. It provides: "When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if: (1) the disclosure is inadvertent; (2) **the holder of the privilege or protection took reasonable steps to prevent disclosure**; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B)." Rule 502(b)(2) clearly makes a privilege holder's level of diligence a factor in determining whether inadvertent disclosures constitute a waiver of the attorney client privilege. Courts are rightly beginning to consider whether a party arguing for Rule 502(b) protection has implemented appropriate technology tools and procedures as an assessment of whether the holder of the privilege took **reasonable steps to prevent disclosure**. *See, e.g., Arconic, Inc. v. Novelis, Inc.* 2019 WL 911417 (W.D. Pa. February 26, 2019); *AdTrader, Inc. v. Google LLC,* 405 F.Supp.3d 862 (N.D. Ca. 2019).

Security for client data is not only in the law firm's and client's best interest, in many cases, in many cases it is the law. Regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act of 2002 impose heightened obligations on companies such as medical providers, financial institutions, and other corporations to secure their customers' and patients' data.



2. Remote Litigation is Not Optional - Do It Securely

To keep pace and comport with professional guidelines, law firms must use technology. But, given the quantity of sensitive data that they possesses, law firms can become targets for bad actors, requiring lawyers and their firms to take great care when engaging in virtual litigation.

How law firms address these risks has important ethical and business implications. Prevention of unauthorized access must the goal. Because Calloquy was conceptualized and built by attorneys, our commitment to information security and privacy – the sort of information security and privacy that only attorneys can understand – is at the heart of all we do.

Build a culture of cybersecurity. Let your partners, your associates, your employees, and your clients know that security is a priority for you. Establish secure systems and provide continuous monitoring to protecting your systems and data. Cybercriminals are continuously evolving – so must you. IT security is a law firm governance issue, not a technology issue. There are lots of strategies and solutions, the most effective ones begin with building a culture of safety.

Train employees to secure their home offices, use secure equipment and networks, follow best practices for remote litigation, including using Calloquy. Teach everyone in your firm how to spot, mitigate, and remediate cybersecurity threats quickly and effectively. Insist that everyone who touches a computer comply with the best practices outlined by your IT team. Keep your employees' operating systems and applications updated. This will help ensure your software is equipped to identify and repel the latest cyberthreats. The most common cyberattacks law firms encounter are ransomware, business email compromises, and "social engineering," or manipulating personnel to divulge key information that would grant access to the firm's network.

Protect and encrypt all audio, video, and screen sharing data when setting up a remote litigation proceeding – client or team meeting, deposition, mediation, or arbitration. Calloquy does this for you. Its case-based approach with tokenized meeting invitations which serve as a deterrent to them being shared, guarding against uninvited guests joining confidential proceedings. This may seem simple, but it's an important step to ensure that your meeting doesn't include any unwelcome participants. Video recordings and transcript files, as well as all stored evidence, are encrypted at rest.

Stage exhibits in a secure vault prior to a deposition in order to collaboratively prepare in a platform that the attorney is already comfortable and familiar with, rather than having to rely on a new platform or service to which they do not have continuous access. Calloquy does this. Calloquy's integrated evidence management allows attorneys and paralegals to upload exhibits where they'll be protected. With most existing court reporting services, attorneys have to rely on a separate third-party evidence platform, which they little familiarity with and gain access to just hours before the deposition starts, increasing the odds of mistakes and the inadvertent disclosure of data.

If you intend to record the deposition for use of video testimony at trial, consult the local rules and alert all parties of this intention when scheduling the deposition. Obtain the requisite consent and make the distinction in your notice of deposition. Calloquy obtains consent to record before each meeting and provides a disclaimer on each participant's window automatically.

In May 2022 a Philadelphia midsize law firm reported that the personal information of 23,066 people was potentially compromised, including customers of the firm's financial institution clients, according to public records following a June 2021 cyberattack.

Calloquy's pre-configured breakout rooms make it easy and convenient to separate the parties for private discussions, whether that's during a deposition, a mediation, or an arbitration. Unlike other platforms that are not built for adversarial proceedings, we prevent people outside of your party, including mediators, from entering your breakout room without advance notice and permission of the attorneys, helping to protect the sanctity of privileged conversations.

Chat without fear. Calloquy's chat features have been purposefully designed to make it possible to safely communicate with your party without fear that your private communications are being inadvertently shared with your adversary or accessed by the meeting "host." Calloquy has worked hard to build a system that saves you from potentially embarrassing mistakes and the risk that can arise when using chat features on mass-market videoconference platforms.

With next-era security features including chat party indicators, breakout room access controls, and auto-locked digital evidence, Calloquy allows you to reliably engage in "full and frank" discussions with clients and colleagues while knowing that those privileged conversations are protected.

One of the most staggering cybersecurity events in 2021 was the ransomware attack on the Colonial Pipeline Co. The attack halted that company's operations for five days and resulted in a temporary fuel supply crunch across the East Coast. Hackers gained access to a VPN account password, granting them access to Colonial's network where they were able take down the company's entire infrastructure.

Ironically, the account and associated password were no longer actively in use, but since the credentials were still enabled, the hackers had access to Colonial's network. The cybercriminals discovered the password in a bundle of passwords on the dark web. Just over a week after their systems were taken down, Colonial received a ransom message asking for about $4.4 million, which they paid within hours.

3. After the Meeting

When participants have logged off, when the court reporter has stopped transcribing, when the mediator has gone home, the exhibits, transcripts, and chats stored on any platform still require safeguarding. Calloquy does this. With the same level of encryption with which it hosts remote meetings and proceedings. Calloquy's case-based management system automatically stores every exhibit, transcript, and piece of evidence created throughout the case from the outset of the case and ensures that every exhibit will be at the ready when you need it.

Calloquy also preserves the authenticity of those new exhibits created during the deposition and arbitration by eliminating the unreliability that happens from asking the witness to annotate a hard copy at their home or opposing counsel's office then inviting them to mail it to the court reporter. Data manipulation and alteration pose a significant risk that courts must not overlook. File format, storage, and transfer methods can impact the integrity of the evidence.

A key component of Calloquy's videoconferencing platform allows attorneys to effectively manage and preserve the evidence introduced and annotated discussed during virtual depositions or arbitrations. Evidence integrity is safeguarded as Calloquy provides customizable exhibit stamps and locks exhibits after they have been introduced. If a witness is asked to annotate a document during a deposition, the attorney conducting the deposition has the option of discarding the annotations (and therefore retaining the original exhibit) or saving the annotated document as a new exhibit, securely preserving those annotations for the records.

All chat messages in the Calloquy platform are ephemeral, meaning there is no permanent record of the chats created. Therefore, meeting hosts are unable to covertly view or download their opponent's chat logs during or after any meeting.

Speech-to-text or court reporter prepared transcripts and video recordings are easily accessible and safely stored in an encrypted repository in the same platform that the attorney uses every day.

Calloquy has created a remote litigation platform which employs gold-standard data security, with transit encryption relying on TLS 1.2 (Transport Layer Security) which utilizes PKI (Public Key Infrastructure), specifically an asymmetric type (use of public & private keys), which is generally considered the gold standard. With respect to end-to-end encryption, Calloquy utilizes the following encryption components: HTTPS, TLS 1.2, WebRTC and underlying components including DTRS-SRTP, and database level encryption (at rest).. Our security management system was developed, is maintained according to, and comports with the ISO/IEC 27001 standard and is regularly audited.

Storage security is implemented for all sensitive client files via strong encryption, with access control implemented within the application layer. Data is encrypted at rest using the AES-256 bit encryption standard. Subsystems that are hosted in the Amazon Web Services cloud environment are equally protected via Amazon's strong facilities controls.

The new era of litigation is here. And it requires remote litigation. Litigate securely with Calloquy.

Remote litigation is changing how you practice law. But Calloquy knows that it's not changing why you practice law.

If you have questions about Calloquy, would like to speak with a customer service rep, or schedule a demonstration, **call 1-855-843-4777**.

View Calloquy's comprehensive guide to rules relevant to remote litigation.

Check the Calloquy blog for updates on remote litigation, Calloquy services, and more.

Calloquy

www.calloquy.com
(855) 843-4777
info@calloquy.com