Don’t be the Lawyer Who Needs a Lawyer

How Secure Video Conferencing Can Reduce Malpractice Risk

]pexip[

Contents

Executive Summary

As COVID-19 shutdown orders were issued in early 2020, attorneys had no choice but to practice "in-house" – literally. This new way of practicing law meant learning how to utilize tools and software already available within the firm or, in some cases, implementing completely new technology.

Without access to in-person interactions with colleagues, staff, clients, and outside counsel, lawyers have turned to video conferencing for business continuity and to maintain relationships with clients and staff. Now, as remote meetings have become the post-pandemic "new normal" for many law firms, the question is no longer *if* lawyers should use video conferencing, but *how* to optimize this tool, both in terms of maximizing productivity, as well as another critical consideration: security.

In September 2020, a federal court hearing on voting machines and election security in Georgia had its own security issues when it was suddenly bombarded with pornography and images of the 9/11 terrorist attacks. According to a CNN report[1] , the interruption happened abruptly about two and a half hours into the hearing, when an individual joined the call by video and immediately began sharing their screen with the disturbing images. More than 100 people participated in the breached call, which was quickly shut down, resuming an hour later.

Bryan P Tyson, a lawyer for the state of Georgia in the case, said he has never seen anything like it. "It just showed the tension we have with open access to proceedings and using technology," he said. "One of those things we have to learn from and grow from."

While this security breach happened during a court hearing, it demonstrates the increased need for awareness of any potential security issues related to the use of such platforms by lawyers as well. Law firms today are in positions where they are hosting virtual meetings with participants ranging from clients, to opposing council, to financial institutions, and sharing highly sensitive information over video in all of these situations. Protecting the attorney-client privilege and maintaining the duty of confidentiality is both a statutory requirement (in most jurisdictions) and an ethical obligation, as well as a necessity for the business.

However, because of the emergency posed by the virus-related shutdowns, many attorneys have not had time to fully consider these concerns when choosing a solution for video collaboration. Video conferencing can be an extremely safe and secure means of communicating, but only if the solution is designed with security in mind. Continued frequent usage of video conferencing for lawyers will require law firms to choose their solution based on its security standards to ensure that their meetings are secure and private, and that confidentiality of client information is maintained. This is of course to maintain the trust of clients and the legal community, but also to minimize their own risk of liability.

Lawyers were asked,

"Which one of the following issues will have the biggest impact on the practice of law during the next five years?"

Their responses:*

34%
Emerging technologies

19%
Corporate governance regulations

18%
Privacy, data, security concerns

12%
Increased globalization

*Top responses shown
Source: Survey of 350 lawyers amongst the largest law frms and companies in the United States and Canada, comissioned by Robert Half Regal and conducted by and independent reserach form

The Importance of Technological Competence in a Remote Environment

Despite the challenges of practicing law in a pandemic, every lawyer's primary responsibility is to protect the interests of their clients, which includes safeguarding their confidential information. Therefore, attorneys must be "technologically competent" while attempting to navigate the hurdles of working remotely. For American lawyers, an attorney's failure to learn how to use available technology, including video conferencing platforms, could violate Rule 1.1 of the American Bar Association's Rules of Professional Conduct[2].

Under the ABA's Rules of Professional Conduct, when lawyers utilize video conferencing platforms or connect to remote servers, they must use secure internet connections, passwords, and dual authentication methods. Unfortunately, some attorneys have found themselves at the mercy of the platform's security (or lack thereof). One potential scenario:

Scenario A

When the COVID-19 pandemic hit, Lawyer A chose one of the most popular video conferencing platforms. Unfortunately, they were one of 500,000 users who had their account information stolen and exposed on the dark web3 in March 2020, potentially subjecting them to greater risk of a malpractice claim.

Scenario B

Lawyer B thoroughly analyzed the various video conferencing platforms available (including their potential for breaches) and chose another platform to handle the firm's video conferencing requirements. As a result, this attorney has experienced no breaches, hacks, or leaks and continues to manage cases securely, with no significant increase in liability risk.

When selecting a video conferencing platform, a law firm should review the software's features and conduct sufficient due diligence on the security procedures of any system that will transmit confidential client information. They should also verify whether the platform uses encryption and password protections and research whether the service has already been subject to data breaches.

Evaluating Video Conferencing – With a Security Mindset

According to a survey of 175 lawyers working in the largest companies in the U.S. and Canada commissioned by Robert Half Legal, eight out of 10 lawyers surveyed said their collaboration with IT specialists has increased in the past two years. Although video conferencing has been around for decades, only a fraction of businesses regularly used these platforms just a few years ago. The legal industry is well known for being technology adverse. However, video conferencing, virtual court hearings, remote meetings, and virtual depositions are undeniably part of modern law practice.

Today, it is not enough for a lawyer to simply be comfortable with using such technology; they must be able to facilitate its use independently by being familiar with several primary functions:

Hosting

One user must "host" the meeting while others can attend as participants. The host controls the meeting and must furnish the software licensing, while the participants can access a free version of the application or join through their web browser.

Screen sharing

Most video conferencing software allows two parties to share audio and video of themselves in real-time, meaning that the host typically allows the other participants to view the presenter's computer screen.

File sharing

For attorneys, file sharing capabilities during a video conference is often critical, particularly during hearings. The main concerns with file sharing are whether the confidentiality and integrity of the file data are ensured during the session, through methods such as military-grade encryption and access control.

Chat

Most video conferencing platforms enable participants to share text-based messages that allow users to comment, share URLs, or ask questions during the meeting. These chats should be considered public conversations with no expectations of confidentiality. They are part of the client file and should be retrievable and archived as such.

When deciding which platform is best for your firm, you should assess the scope of your needs, review functionality, and explore various products. Also, consider this: free versions of video conferencing platforms for attorneys do not usually provide all the critical features of the complete system[4].

Security Features to Look for in a Video Conferencing Platform

Not all video conferencing providers are created equal. When evaluating vendors, make sure you ask the right questions and understand how your meeting data will be protected. Below are a few areas to consider:

End-to-end encryption.

No platform can be completely immune from potential cyber hacks or breaches. However, the service should include end-to-end encryption and operational security control capabilities such as multi-factor authentication, certificate-based identity management, session-centric access control, and any other industry-standard features that will help secure meetings. For example, features such as requiring a password to enter a forum and placing participants in a "waiting room" pending approval for admittance should be enabled.

Control over data.

Do you know where your meeting data lives? Look for a video conferencing provider that is transparent about their corporate data policies and provides solutions that give you ultimate control over your information. With a privately-hosted deployment, you can run the entire meeting platform on-premises and inside your network, or on any private cloud you choose. You'll benefit from all the security measures you already have in place, plus those in place by your cloud provider. By establishing these policies and practices up front, you minimize liability risk down the road.

Ease of management with security built in.

Want the security benefits of a self-hosted solution, but don't have the staff to manage it yourself? Consider a solution that provides the data control and transparency of a self-hosted software deployment with the ease and scalability of a SaaS solution. Or, if using a SaaS solution, make sure it uses information security best practices and complies with risk management standards such as ISO/IEC 27001, SSAE 18, SOC 2, or NIST SP 800-37.

Privacy controls.

Look for the option to protect access to your Virtual Meeting Rooms using PINs, certificate validation, directory lookups, or other authentication and authorization mechanisms for an additional layer of security. As the data controllers for each session, meeting hosts should have mastery of all information access mechanisms, including room locks, mute controls, and full participant oversight. If your organization isn't comfortable placing this responsibility with session hosts, implementing an conferencing policy engine can automate these processes either in isolation or in conjunction with global organizational security architectures such as Zero Trust.

One-time-use meeting rooms.

Use randomly-generated aliases that only exist for the duration of the meeting versus static meeting rooms that are always available. This minimizes the attack surface for adversaries and encourages automated distributed mechanisms, further protecting your clients' most precious assets – their data.

Customizable, branded interfaces.

Choosing a platform that allows firms to add their logo and branding the waiting room and meeting room screens puts clients and other guests at ease. Participants get a feeling of security and peace of mind knowing they're in the right place, and the overall experience promotes a secure workflow.

Because of the sensitive information that might be shared during a video conference meeting and considering the fiduciary duties that lawyers owe to clients, attorneys are obliged to review the security and privacy policies of any video conference service they use. The review should pinpoint the scope of security and privacy considerations, as well as any potential data mining risks. They should also know how the data is permitted to be used under the platform's terms of use. In addition, lawyers must relay to clients the scope of security and confidentiality that accompanies video conferencing between attorneys and clients under the platform.

The creation of potentially discoverable data is another critical consideration to make. For example, video conferencing can be an excellent tool for conducting group meetings such as mediations, which might not raise confidentiality or protection issues. However, using these platforms to conduct interviews with clients and consulting experts could be viewed as discoverable.

Under the Federal Rules of Civil Procedure, a party must produce information in response to a proper request. According to Federal Rule 34[5], "any designated documents or electronically stored information" must be produced. The rule is intended to cover all current types of computer-based information and is flexible enough to encompass future changes and developments, meaning that a video conference recording is likely discoverable, and a firm that does not address the proper use of video conferencing could face a host of liability issues.

Further, Model Rule of Professional Conduct 1.6[6] states that lawyers must make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 8 to Model Rule 1[7] explains that, to maintain the required knowledge and skill, lawyers should stay abreast of all changes "including the benefits and risks associated with relevant technology."

Fortunately, certain features of video conferencing platforms enhance security and help minimize the risk of legal malpractice claims. Therefore, when considering a video conferencing solution, firms should perform a risk assessment or research the guaranteed standards and choose a platform that upholds high security, privacy, and transparency standards for clients, partners, and employees. This is especially relevant for firms that work with government and healthcare clients. S mechanisms that organizations should consider in video conferencing platforms include:

- GDPR, ISO/IEC 27001:2013, and U.S. Department of Defense Approved Product List (APL) certification
- Federal Information Processing Standard (FIPS) 140-2 validation and Health Insurance Portability and Accountability Act (HIPAA) compliance
- SOC2/SSAE18 compliant data centers

Highly secure platforms also routinely feature enhanced documentation options, no download or software requirements, no prerequisite internet connection when self-hosting, multiple integration options, and secure data storage. A video meeting room for attorney and client communications separate from the court is also an important feature. Additionally, firms should be wary of platforms hosted in another country.

Generally, platforms that do not require a password that is known only to the users should be avoided. However, a program that enables the host to limit recording by others seems essential. In addition, a firm's in-house data experts should identify the most secure options available and track innovation that creates other encryption and security features. Finally, a firm should make it a policy that users who prefer to use other software will not do so.

Tips to Mitigate Risk When Using Video Conferencing

Video conferencing is a powerful tool that has helped firms practice law during the pandemic, when on-site meetings were not feasible. The proven efficiency and cost-savings opportunities of video conferencing mean that the frequent use of remote meetings will continue post-pandemic for many law firms.

However, due to security and liability concerns, not all lawyers are comfortable utilizing video conferencing tools. Moving forward, firms need to ensure that this technology is working for them and not setting them up for exposure to liability issues.

Many of these platforms can be used safely in the legal industry if steps are taken to increase the security of meetings. Here are some tips to minimize risk and avoid becoming the subject of a malpractice claim:

Always use a password.

Requiring a password to enter a meeting helps ensure that only those with the meeting ID and password can be present. For increased security, remove the password from the email invitations and forward it to invitees separately.

Know the platform.

Even a seasoned professional using their technology platform of choice should spend some time familiarizing themselves with its functions to make sure they know exactly how it works before the meeting begins. Particular attention should be paid to ensure that case notes and other confidential information are not accidentally shared.

Follow the rules.

Several organizations have published video conferencing guidelines for lawyers. In California, LACourtConnect has an 81-page user guide, the American Arbitration Association has a six-page "Model Order and Procedures for a Virtual Hearing via Videoconference," and JAMS put together a multipage "Videoconferencing Guide." Understand procedural requirements. The in-person procedures for identifying, marking, and admitting exhibits will most likely need revision for the virtual environment.

Monitor attendance.

Consider authenticating meeting guests before they can participate and lock the meeting once all expected participants have joined.

Remember to mute.

Regardless of what platform you choose, always assume you have a hot microphone, even though you appear muted on the screen.

Disable unnecessary functions.

To avoid having private information saved on your video conferencing platform, consider disabling chat, screen sharing, annotation, and whiteboard functions. If you are concerned about sharing files in a meeting, distribute documents another way.

Ensure that you are disconnected.

If you close your laptop but still have a connected monitor, you should assume that your microphone is still on.

Record with caution.

All parties need to agree regarding whether recording of the meeting will be allowed, and if it will be, determine any limitations on the creation and use of the recording. Also, be aware of where recordings are stored – cloud, computer, servers, or some combination thereof. If you do not need to record the videoconference, consider turning off any automatic recordings to preserve confidentiality and save storage space.

Close unnecessary applications.

All meeting participants should close all unnecessary applications, files, and browser tabs before entering a video conference so that confidential client information is not inadvertently exposed during screen sharing. In addition, you should suppress notifications and pop-ups, and no participants should join a meeting with their email open in the background.

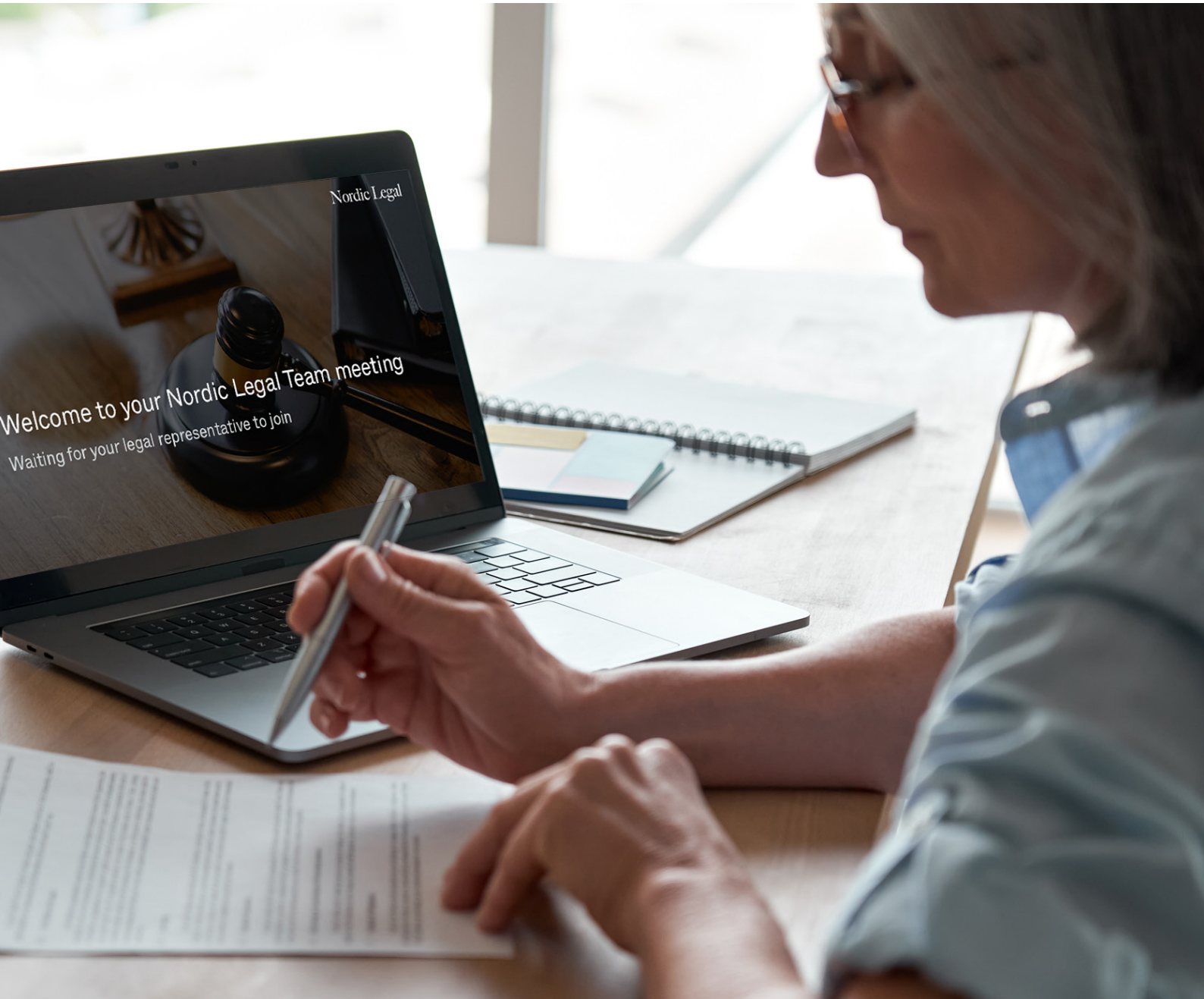
Despite the best efforts, managing the risk of malpractice claims can be highly challenging. The process of mitigating risk should include constant and transparent client communication – both in-person and remotely via a robust video conferencing platform – along with timely and honest evaluations of what can be achieved throughout the representation.

Conclusion

With the rise in remote work and virtual court proceedings, security is more important than ever. Pexip is committed to upholding high information security standards, privacy, and transparency for its customers, partners, and employees. Pexip offers security-first, enterprise-grade video conferencing solutions using industry-standard encryption and security protocols to maintain confidentiality.

To find out why some of the world's largest companies and public organizations trust our platform for their video conferencing needs, visit:

pexip.com/legal



References

[1]Leah Asmelash, “A federal hearing was interrupted with images of 9/11 and pornography,” (September 2020) CNN, retrieved 27 August 2021 from. https://www.cnn.com/2020/09/14/us/georgia-hearing-zoom-bomb-trnd/index.html.

[2]American Bar Association (2021). Text of the model rules of professional conduct. ABA, retrieved 25 August 2021 from http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html.

[3]Davey Winder, “Zoom Gets Stuffed: Here’s How Hackers Got Hold of 500,000 Passwords,” (2020), retrieved 24 August 2021 from https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/?sh=1f0f67ac5cdc.

[4]Fed. R. Civ. P. 34(a), retrieved 26 August 2021 from https://www.law.cornell.edu/rules/frcp/rule_34.

[5]Fed. R. Civ. P. 1.6., retrieved 26 August 2021 from https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/.

[6]Fed. R. Civ. P. 1.1., retrieved 26 August 2021 from https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/.

Sources

AAA-ICDR Model Order and Procedures for a Virtual Hearing via Videoconference. American Arbitration Association, 2021

Asmelash, Leah. A Federal Hearing Was Interrupted with Images of 9/11 and Pornography – CNN

Future Law Office 2020. Robert Half Legal, 2020

LA CourtConnect User Guide. LA Court, 2020

Model Rules of Professional Conduct. American Bar Association, 2021

Rule 1.1 Competence - Comment. American Bar Association

Rule 1.6: Confidentiality of Information. American Bar Association

Rule 34. Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes, Federal Rules of Civil Procedure

Using Videoconferencing to Settle Your Mediations Remotely.” JAMS Mediation, Arbitration, ADR Services, 2021

Video Conferencing for Lawyers Reviews (2021) | Lawyerist

What Lawyers Should Do When Using Video Conferencing. Klemchuk, 2020, https://www.klemchuk.com/ideate/video-conferencing-for-lawyers-security-privacy-concern

“Zoom Gets Stuffed: Here’s How Hackers Got Hold Of 500,000 Passwords.” Forbes, Forbes, 28 Apr. 2020 - https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/?sh=1f0f67ac5cdc

]pexip[

www.pexip.com