What You Don't Know Can Hurt Your Client:

Why You Should Care Who Sees Your Deposition Transcript Before It's Delivered

By Jamal Lacy, Juris Doctor 

So you're in a rush to find a court reporter for a last minute deposition. Somehow, after spending a day searching with no success, you finally luck into securing a reporter on short notice. Now, we've already discussed the headache of court reporter shortages, long turnarounds, and add-on fees. But there's another elephant in the room you might not have considered.

Here are a few questions for you . . .

When you hire a court reporter is there a security plan? Does that reporter have a completely different plan than the agency that made the assignment

in the first place? What obligations and responsibilities do either have with respect to your client's sensitive information?

It's important to ask these questions because they point to a blind spot. Just how secure is your transcript? Think about it. Your client shares personal, private information while a reporter records every word. You spend hours in deposition to produce a transcript that you don't see for weeks. Well, what happens to that information over the course of a two-week turnaround? Where is it stored? Who has access to that information? Most importantly, if your client asked for assurance, could you honestly say the transcript is secure?

Probably not.

Chances are, most lawyers don't stop to consider a court reporter's stance on HIPAA. They might not have a heart-to-heart talk about protected health information or share stories of SOC 2 certification. And when you're rushed to find a reporter with only hours to spare, you probably don't think to look for a written information security plan.

But maybe you should.

Why? Well, that deposition is just one of many gateways to your client's sensitive data. It should go without saying, but your client's information is a prized trophy for any aspiring cybercriminal. And according to the American Bar Association, law firms with a wealth of information and less-than-ideal protection are preyed upon for this very reason:

> *"Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information*

that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client."[1]

So it shouldn't be surprising that a 2021 survey by the American Bar Association found 25% of respondents fell victim to a data breach that year.[2] Even more concerning, a 2019 American Bar Association survey reported that 19% of respondents couldn't even say whether they had suffered a security breach or not.[3] The larger the firm, the greater the uncertainty.[4]

So add cybersecurity to the list of duties that demand your attention. Choosing a new service provider raises a host of questions. Is this safe? Is this reliable? What happens to my information? Yes, it's a lot to consider when you're scrambling to find a stenographer hours before a deposition. But security, no matter how inconvenient, is an unavoidable subject in the legal community. You'd probably hope that a court reporter is just as concerned about these issues as you are. Cybersecurity is a daunting task, but you shouldn't have to go it alone.

[1] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf.
[2] Ries, David, G. "2021 Cybersecurity." American Bar Association, 22 Dec. 2021, https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/.
[3] Loughnane, John G. "2019 Cybersecurity." American Bar Association, 16 Oct. 2019, https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity2019/.
[4] Id.

You should expect as much. After all, your professional expectations continue to evolve as technology expands. Being an attorney entails much more than legal advice. Beyond the billable hours is the trust clients place in your judgment. Technology has brought new opportunities and benefits to the legal industry. But it's also come with new questions, threats, and concerns that influence attorney responsibilities. Throughout the country, state codes of professional conduct now require a certain level of familiarity with legal technology, a new reality that has seen 40 out of 50 states adopt a duty of technology competence for practicing attorneys.[5] This evolving standard of care addresses new practices by drawing upon pre-existing duties of competence, communication, and confidentiality.[6] It's a concept that also dovetails with principles of continuing legal education. In fact, Comment 8 to the Model Rules of Professional Conduct 1.1 states that requisite knowledge and skill includes an understanding of technology and its impact on legal practice:

> *"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."*[7]

Such competency allows attorneys to make the right decision when choosing a service provider. Attorneys should exercise "due diligence" when assessing a prospective vendor and take a fact-specific approach when making their decisions.[8] Attorneys should consider a vendor's security policies, protocols,

---

[5] Ambrogi, Robert J. "40 States Have Adopted the Duty of Technology Competence." LawSites, https://www.lawnext.com/tech-competence.
[6] Ries, *supra* note 2.
[7] Model Rules of Prof'l Conduct R. 1.1, Comment 8 (2020); See also, Ambrogi, *supra* note 5.
[8] Formal Op. 477R (2017), *supra* note 1.

and use of confidentiality agreements.[9] Attorneys should also consider security with respect to virtual practices and risks of inadvertent disclosures.[10] And when using a video conferencing platform, attorneys should choose a service that is consistent with their ethical obligations.[11] Access control, passwords, and confidentiality are major considerations as well. As noted by the American Bar Association:

> *"Access to accounts and meetings should be only through strong passwords, and the lawyer should explore whether the platform offers higher tiers of security for businesses/enterprises (over the free or consumer platform variants). Likewise, any recordings or transcripts should be secured. If the platform will be recording conversations with the client, it is inadvisable to do so without client consent, but lawyers should consult the professional conduct rules, ethics opinions, and laws of the applicable jurisdiction. Lastly, any client-related meetings or information should not be overheard or seen by others in the household, office, or other remote location, or by other third parties who are not assisting with the representation, to avoid jeopardizing the attorney-client privilege and violating the ethical duty of confidentiality."*[12]

This is all to say that your service provider must have a tested security plan. As reported in a 2022 law firm data security guide by the legal tech company CLIO, law firms remain a high target of cybercrime due to the wealth of client information they possess.[13] A firm should take precautions when choosing a

---

[9] Id.
[10] Formal Op. 477R (2017), *supra* note 1; ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 498 (2021), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf.
[11] Formal Op. 498 (2021), *supra* note 10.
[12] Id.
[13] Matich, Teresa. "2022 Law Firm Data Security Guide: How to Keep Your Law Firm Secure." Clio, https://www.clio.com/blog/data-security-law-firms/.

service to handle that information. In other words, Clio urges attorneys to vet their vendors.[14]

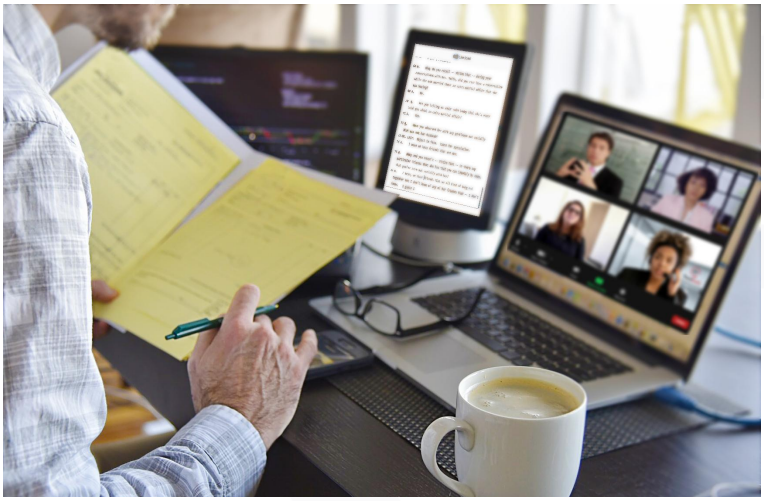
And time is of the essence. This focus on technology competence fits an overarching direction of stricter standards and protections for consumer data privacy across the country. Most recently, Congress drafted a bicameral piece of legislation for a national privacy law named the American Data Privacy and Protection ACT ("ADDPA").[15] This comes as individual states are currently enacting data privacy laws that place more power in the hands of the consumer and more responsibilities on the part of those collecting sensitive data. At the time of this article, California, Colorado, Connecticut, Virginia, and Utah have already passed their respective state data privacy laws. And this is just the beginning as five other states have active bills in the pipeline as well.[16]

What's in these bills? At the publishing of this article, seven states either currently impose or propose to enact risk assessment obligations on businesses collecting sensitive data.[17] Three states currently have or propose to enact a private right of action in the event of a breach.[18] And, as of 2020, 25 states, as well as Washington D.C., require companies to enact their own written information security plans (WISP) when handling private data.[19] The message couldn't be any clearer. When it comes to protecting sensitive information, anyone that handles your client's sensitive information *must* have a security plan.

---

[14] Id.
[15] See Gavejian, Jason C, et al. "Congress Releases Draft Federal Privacy Law with Potential Traction To Pass." The National Law Review, 23 June 2022, https://www.natlawreview.com/article/congress-releases-draft-federal-privacy-law-potential-traction-to-pass.
[16] Lively, Taylor Kay. "US State Privacy Legislation Tracker." The International Association of Privacy Professionals, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[17] Id.
[18] Id.
[19] Minahan, Bill. "What is a written Information Security Program (WISP)?" aNetworks, 11 Dec. 2020, https://www.anetworks.com/what-is-a-written-information-security-program-wisp/.

Attorneys are heeding the call. They're not taking a leap of faith when it comes to safeguarding their information. In fact, they're digging deeper when choosing a vendor. Sure, it's one thing to require a security plan. But how can attorneys judge that plan's effectiveness? An important question for sure. Perhaps that's why some are demanding SOC 2 certification.[20] SOC 2 certification is a voluntary assessment standard created by the American Institute of CPAs that focuses on secure customer data management.[21] The certification process utilizes third-party audits to examine the Trust Services Criteria of security, availability, processing integrity, confidentiality, and privacy.[22] More specifically, SOC 2 compliance identifies four steps to protect data: access controls, change management, system operations, and risk mitigation.[23]



So where does Readback fit into all of this? Well, when we started this journey, our focus was simple . . . to meet your expectations. So we listened to our clients and used that information to fill a void in the court reporting industry. But we also know that some expectations go without saying, which is why our commitment to client satisfaction goes beyond listening. Readback is a forward-thinking service. So it's only right

[20] Vogel, Peter, "Lawyers Need to Review SOC 2 Audit Reports!" Foley & Lardner, LLP, 21 Apr. 2021, https://www.foley.com/en/insights/publications/2021/04/lawyers-need-to-review-soc-2-audit-reports.
[21] "What is SOC 2 Compliance?" Check Point, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-soc-2-compliance/.
[22] Id.
[23] Id.

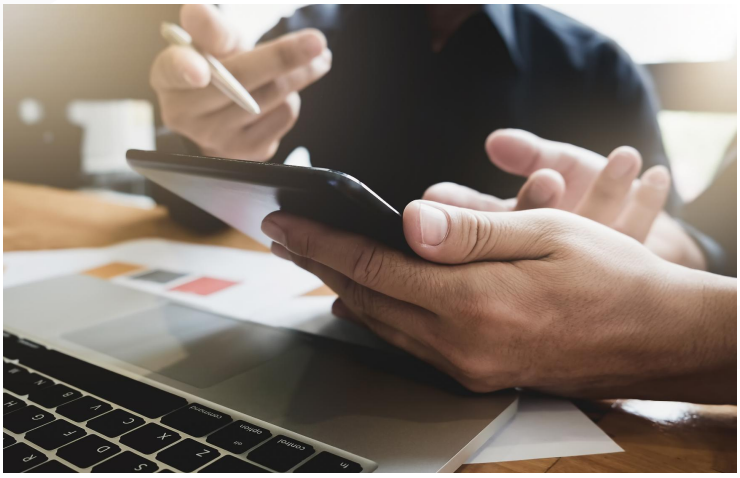
that we take that same forward-thinking approach to your security as well. The fact is, you already have a lot to deal with. We're here to help, not add more to your plate.

You can be confident in knowing that Readback's parent company, InfraWare, Inc., is SOC 2 certified. You should also know that we take principles of confidentiality and access control very seriously. When you schedule a Readback deposition, access to the remote proceeding is controlled by session identification and a password. Participants are given this information ahead of the deposition to log into their Zoom meeting. Upon logging in, participants are placed in a virtual waiting room, at which point our trained Guardian will admit them into the proceeding.

Additionally, Readback's team-based structure affords more control and oversight for your information throughout the deposition process. Ensuring your data security can be a lot for one person to handle. It often involves multiple independent parties exchanging your information, raising security concerns each step of the way. Fortunately, Readback's chain of possession is simple and in-house. Our Guardians and transcriptionists are trained employees, which means you don't have to worry about unknown third parties handling your information. This might not always be the case with freelance court reporting. The court reporter you hire might be an independent contractor with his or her own security plan . . . or maybe no plan at all. This means that confidentiality and access to your client's sensitive information could vary depending on who is assigned to your case.

Finally, Readback's parent company, InfraWare, has extensive experience in medical transcription. This means our company is familiar with meeting the high expectations and requirements of safeguarding personal health information and personally identifiable information, and complying with HIPAA regulations. InfraWare is no stranger to confidentiality, WISP

requirements, and business associate agreements to maintain client confidence. This accounts for a company-wide standard that we set for security, a standard that we take very seriously. Can you say the same about that last-minute court reporter you just hired?



Listen, security might not be a flashy topic. But it's our most crucial obligation to you. We understand that service companies like ours play an important role in your protection. Yes, Readback is committed to providing a simpler, more empowering, and more convenient approach to your deposition experience. But convenience should not come at the expense of security. Let Readback provide the best of both worlds.