The United States Law Week

INSIGHT: Covid-19 and E-Discovery—Transitioning Remote Document Reviews

By John E. Davis and Rochelle-Leigh Rosenberg

May 12, 2020, 4:00 AM

In Part 2 of a two-part series about planning for security and quality challenges with remote document reviews, Crowell & Moring attorneys discuss processes and workflows for securely staging and managing a remote workforce, including strategies for handling particularly sensitive information, and steps counsel may take to mitigate remote review risks.

Document reviewers eventually will be permitted to return to their offices, but this transition will likely be gradual and uneven, metered by varying circumstances. Many reviews will continue in this remote construct, for continuity purposes and as processes and concerns get addressed and economies are realized.

Companies with instant review requirements and those contemplating their future needs should start planning now, thinking of the flexible strategies discussed in this article series to protect confidentiality and accomplish review objectives.

Creating a Customized Review Plan: Hiring and Training

The individual may be the linchpin, or the weak link, in the confidentiality chain constructed for remote reviews. Providers should be able to explain in detail how their managers and reviewers are screened, hired, and supervised in these changed circumstances. Ask the provider:

- What process is followed to identify qualified individuals and to screen out potential bad actors and performers?
- How are background checks, diligence and interviews conducted remotely?
- Does the provider use W2 employees or contractors (or both)? What is their average tenure with the company?
- Are reviewers hired from the same locations where brick and mortar review facilities exist, or sourced more broadly? That may be an important factor when facilities are permitted to reopen, and there is the option to switch back to traditional in person review and oversight.

Training too can make the difference between success and underperformance here. Ask the provider:

- How it trains document reviewers on proper security protocols?
- Are reviewers instructed to exclude others, cell phones, camera/recording devices, Alexa and Google minis from the review space? To use privacy screens?
- Are reviewers instructed not to discuss confidential information where it may be overheard, and not to leave an open application unattended?
- Are reviewers trained to respond to, and report, threats such as phishing attacks?
- If it performs regular check-ins and refresher training for reviewers, gathering lessons learned and reinforcing appropriate processes?
- How it logs activity in the event of an improper disclosure?

The plan also should address what happens when the engagement is over. Reviewers need to return all training materials and destroy any home notes or other vestiges of the confidential information in their possession.

Creating a Customized Review Plan: Oversight

From lack of proper equipment to the distractions of roommates, children, home schooling, pets—the list goes on, remote review demands different approaches to promoting quality and efficiency. The plan needs to confront these new challenges and address how managers are ensuring consistency, quality, and productivity of remote workers.

Ask how managers are checking on the health and wellness of reviewers, consistent with HR and public health laws. Are accommodations made for the increased home commitments that can undermine review objectives? Further, address what programs and technology are used to monitor reviewer activity, spot outliers and distinguish productive workers from those who just appear busy.

Slow internet access—from the platform provider, or the local reviewer—may undermine the best planned review. Some providers must game plan for hundreds of reviewers simultaneously logging in from different locations. A high volume or intensity matter may require work to be staged during time periods of lesser internet demand to avoid crippling lags in database performance and home Wi-Fi. Ask for reports on standard productivity measures and expectations under normal and work at home circumstances, and strategies to adjust to meet demand.

Designing Appropriate Workflows for Information of Varying Levels of Confidentiality

Clients and counsel need to understand their risk thresholds as to particular types of confidential information involved in a review, and ensure the plan includes controls tailored to those risks. Some matters may involve information of such sensitivity that the risks of home review are unacceptable.

For many companies, however, a combination of role and location based access restrictions may prove sufficient. Some options include limiting access to information of elevated sensitivity to:

- specially vetted persons;
- outside or inside counsel;
- designated locations (e.g., onshore vs. offshore); and
- particular IP addresses and points of access.

If certain documents may only comfortably be reviewed on company premises, counsel should consider ways to postpone review until after the crisis passes. Be aware that each of these restrictions may impact review pace, quality, information sharing and costs, and plan accordingly.

Additional Steps to Advance Information Security

Counsel may also take additional steps to mitigate the risks of remote reviews.

First, thoughtfully culling datasets before giving remote review teams access will reduce risks of data being exposed, mishandled or misevaluated, strains on remote systems, and costs of review. Further consider categorizing data (including by confidentiality type) for routing to reviewers and locations appropriate to the goals of the review and the risks presented.

Second, counsel should review and update provider contracts, including permitted locations of work, roles and responsibilities, security and privacy schedules, rules regarding cross-border access, and indemnification language, to make sure remote review risks are appropriately addressed.

Third, your interest in data security and confidentiality does not end at its production. Counsel also should ensure appropriate confidentiality and data protection agreements with receiving parties, who also may need to review the data remotely. Counsel may inquire as to safeguards in place for such reviews, and require adequate assurances that recipients exercise reasonable security measures. These topics may be covered in standard stipulations between parties or court orders, so make sure the forms used are updated with any unaddressed risks in mind.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

About the Authors

John E. Davis is co-chair of Crowell & Moring's E-Discovery & Information Management Practice and a member of the Litigation Group. He has over 20 years of experience as internal and outside counsel representing companies in complex litigations and investigations, and advising clients on information law issues—including discovery, data analytics, privacy, cross-border transfers, cybersecurity, information governance and emergent technology.

Rochelle-Leigh Rosenberg is a counsel in Crowell & Moring's Litigation and Health Care groups. She litigates complex matters in federal, state, and arbitral forums, with a particular focus on commercial health care disputes, class actions, and discovery disputes.