E-Discovery & Legal Tech News

INSIGHT: Covid-19 and E-Discovery—Challenges With Remote Document Review

By John E. Davis and Rochelle-Leigh Rosenberg

May 11, 2020, 4:01 AM

The Covid-19 pandemic has forced document reviews to be staged remotely, often from reviewers' individual homes. In Part 1 of a two-part series, Crowell & Moring attorneys discuss the need to create an informed plan to address particular risks and features of remote review, including questions to ask about security in the physical environment of the review and technology used to deliver and access company information.

The Covid-19 pandemic has upended the usual operation of document reviews and scrambled settled expectations as to their conduct.

Previously, teams of reviewers typically would work in office settings on company equipment, under the immediate supervision of counsel and managers working from established playbooks for security and oversight. Now, health and safety requirements have forced most reviewers to work remotely.

This new environment presents different challenges to information security and review quality. Companies and their counsel must carefully consider their needs and risk tolerances when adapting to these evolving circumstances, while meeting their confidentiality and production obligations.

Create a Plan Based on Your Security and Operational Needs

Rather than immediately jumping into the deep end of remote review, counsel, clients and providers (data and review) should communicate their requirements and work together to create a tailored plan.

Providers may already have a contingency plan on the shelf, but that may not address client specific needs and likely has not been tested under the extraordinary circumstances we see today. The plan should at minimum address information security, remote staffing, training and oversight, and workflows for different types of confidential information handling.

In particular, ensure the plan is consistent with company data and vendor management policies, which may be silent on, or conflict with, remote review. For example, some clients may require a physical inspection of review sites before permitting vendor engagement or access to certain types of information.

Indeed, some companies require a "clean room" with security guards, badge or key pad logins, cameras, phone lockers and other hard coded safeguards. Home worksites of third-party reviewers would hardly qualify. The policies may need to be re-evaluated. When remote work realities are incompatible with immovable company requirements, production expectations and deadlines may need to be adjusted.

Physical and Technology Security

Consider how the remote workforce is assembled and enabled to practice effective security procedures. Asking the following questions can advance the tailoring of an appropriate review plan.

1. In what physical environment will work be conducted?

The plan should address the permitted locations of remote review, and the persons and equipment permitted in the review space. Ask the provider:

- What is a permitted workspace?
- May third parties occupy the same workspace?
- What exceptions are made for co-residents?
- What is the policy on reviewers' cell phones and cameras in the space?
- Are additional safeguards (such as headphones and privacy screens) required so that any bystanders, passers-by, roommates, security cameras, etc., cannot see or hear privileged and confidential communications?
- How are the requirements enforced? Is compliance just a matter of instruction, or will there be, for example, photographic documentation and video check-ins to assess compliance?

2. What secure means of data access are used?

Technical controls should work in tandem with physical restrictions to maintain privilege and confidentiality. Ask the provider how it regulates access for the various actors involved in a remote review:

- Does the provider use a Virtual Private Network or other secure access programs (like Citrix) to maintain privacy and security?
- Does the credentialing protocol meet industry and company requirements for security? For example, does remote access require single or multifactor verification, and how?
- How does the provider ensure programs are up to date, with needed patches?

Ask further if there are restrictions on access points. For a home review, some companies may wish to limit access to registered IP addresses tied to the reviewer's home address, to better control the environment and limit opportunities for unauthorized views from unfamiliar locations. One size does not fit all, however, and such restrictions probably are not appropriate for outside counsel and managers who require different access points and mobile access even when reviewers are staying at home.

3. What technology is authorized and used in the review?

The device used to review documents may advance security and performance, or open up unacceptable gaps in protections and workflows. Ask the provider:

- May reviewers use personal computers, or does the provider distribute dedicated, locked down machines like thin-client devices, with physical and software restrictions and up to date protections?
- What are the technical and procedural restrictions on reviewers' ability to use, download, copy, print, or export files from the review database? Can reviewers use USB or other external drives? Take screen shots? Copy/paste information to another application? Best practices call for remote review environments to be self-contained in the secure application, with exceptions only for specified roles and circumstances.

The technology used to oversee remote reviews is equally important. Many providers use video conference services, including "free" services that may lack proven security and privacy controls and track records. Gain an understanding of how team communications, calls, updates to processes, and training is being conducted. Make sure the tool's privacy policy is understood, and that functionality for accessing, recording, screen sharing and forwarding calls/videos and related information is locked down to designated managers for defined reasons, with logging.

In Part 2 of this series, we will discuss strategies and workflows for securely staging and managing a remote workforce, including handling particularly sensitive information, as well as additional steps that counsel may take to mitigate remote review risks.

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.