# Returning to a New 'Business as Usual': What it Means for Your IG and E-Discovery Obligations

Addressing information governance and e-discovery considerations may appear daunting—or even impossible—because very few companies are prepared for a crisis of this magnitude. As the country reopens, your company should act with this in mind.

By **Diana M. Fasching and Leslie A. Gutierrez, Redgrave LLP** | June 08, 2020

Today's reality amidst the COVID-19 global pandemic is uncertain, even as we gear up towards a return to the new "normal." Bars and restaurants are reopening, social gatherings are beginning again, and people are returning to work. But as companies move back into offices, or permanently transition to new remote modes, actions surrounding your information governance and e-discovery obligations need to be addressed more completely than ever.

Now is a critical time to assess what may have gone wrong in the way of information governance during such turmoil and how to right the ship by adhering to, and bolstering your existing information governance and e-discovery policies and procedures.

## Data Management Risks

Regardless of how effectively your company has been running "business as usual" during the pandemic, data management efficiencies have been negatively impacted. Large portions of the workforce, many of whom may have never worked from home and may be unfamiliar with company telecommuting policies, have continued to create, share, print, and store company documents while at home.

While most are doing so on company-issued devices, and hopefully, while logged into a VPN or similar protected network, some employees may have resorted to using personal devices and personal email accounts for work purposes at home during the peak of connectivity issues. Some may have even been forced to save documents to their personal devices or local hard drives rather than secured shared drives on company networks. And even company supported new platforms, such as Zoom, to facilitate business, have presented new risks.

All of these new ways of creating, sharing, and storing information increases the potential for files to be lost or deleted, and for unauthorized users to access or alter sensitive business information, especially when divorced from any information governance policies or oversight.

## Data Security Threats

While many companies have taken steps to add more robust security and protection of their networks over the past years, the mass exodus of employees from office to home has likely stressed these protected networks. Early on, companies faced questions as to whether their VPN networks could handle the shift. For one, the potential for employees to work outside the security of their company's protected networks poses

significant risks to data privacy. If companies were forced to fast-track rollout of untested technologies, such as new videoconferencing applications, serious security flaws may have been overlooked that could impact confidential information of customers and/or employees that has been shared across those platforms.

Cybercriminals are ready and waiting to exploit any weaknesses uncovered during this pandemic. Phishing scams remain omnipresent, with emails related to stimulus checks and stay-at-home orders as tempting clickbait, especially among employees who are more distracted than usual by cohabitating family members. The potential for these flaws and vulnerabilities to expose your company and your information systems to serious cybersecurity threats is high.

## Litigation Concerns

Preservation of documents that are or will be subject to a legal hold is another significant concern. With an entire workforce operating from home, there is the potential that documents have been accessed, created, and stored in ways or locations not directly controlled by your company. If company documents exist in locations unknown to the company, locating documents that may be subject to a future legal hold could be a challenge.

Also, thousands upon thousands of employees have been furloughed or laid off, some never to return. Has your IT team taken all necessary steps to preserve those employees' data as needed? Standard procedures that may be dutifully executed in the ordinary course of business may slip through the cracks in such discombobulated circumstances.

## Defensible Disposition Projects

More likely than not, your company is showing a renewed emphasis on trimming costs wherever feasible. Under normal circumstances, no one debates that it is a good idea to get rid of legacy and orphaned information no longer needed for business operations, record retention, or legal holds. However, amid an economic upheaval of global proportions, defensible disposition projects are even more at risk of languishing from lack of stakeholder sponsorship and funding, even though excess retention of outdated information has substantial costs as well as latent risks. When your company is struggling to keep operations afloat and looking to trim costs, legacy and orphaned information provide a rich target for potential cost savings that can also improve information governance compliance.

## Steps to Take Now

Addressing the above considerations may appear daunting—or even impossible—because very few companies are prepared for a crisis of this magnitude. As the country reopens, your company should act with the following in mind.

First, it is imperative that you do not desert your existing information governance and e-discovery policies, even in the wake of non-compliance. Demand compliance with processes and systems in place, even if they were all but abandoned at some point in the pandemic. Those policies, and your company's adherence thereto, put you in a place of compliance to begin with.

Second, develop new policies or mandates directly addressing problems that may have arisen during the sudden (and potentially permanent) transition to remote work. For example, consider issuing questionnaires to employees about such things as whether they stored company information on personal devices. Instruct employees who have printed documents at home to bring them in for proper filing or shredding. If needed, prepare inventories of data not on the company network that may need to be collected and preserved. Send a notice to all impacted employees to remind them about their specific preservation obligations. Identify the issues and act accordingly.

Third, consider whether the circumstances of fundamental shifts in employee workforce numbers and alignments presents a good opportunity to address previous information governance deficiencies, including the over retention of outdated information. There are many objectively reasonable motivations for taking action, including protecting employee and customer data, regulatory compliance, and good information stewardship principles.

Fourth, and finally, document your compliance efforts during and after the COVID-19 response. Document the limitations and shortcomings experienced by your company in transitioning to remote work or during the stay-at-home period, including the thinning of resources, the use of untested technologies, or the forced abandonment of certain information system protocols. Documenting everything that impaired your ability to remain compliant with any data governance or e-discovery obligations could help you in the future. Additionally, document everything you are doing and will do to address those adversities. This documentation will help you to establish that you acted as reasonably as possible under these very unique circumstances.

*Diana M. Fasching is a managing director with Redgrave LLP, a national law firm focused on addressing complex legal challenges that arise at the intersection of the law and technology. She is based in Raleigh-Durham, North Carolina. She works collaboratively with clients' legal, business, and information technology teams to understand complex technical systems and infrastructures and to address discovery and information governance needs. Diana can be reached at dfasching@redgravellp.com.*

*Leslie A. Gutierrez is an attorney in the Chicago office of Redgrave LLP and focuses her practice on matters concerning e-discovery and information law. Her work includes drafting and negotiating ESI protocols, drafting legal briefs on e-discovery related issues, interfacing with IT professionals, drafting search protocols, overseeing large document review projects, and working on complex litigation matters. Leslie can be reached at lgutierrez@redgravellp.com.*