Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Adapting Information Governance For The COVID-19 Era

By **Scott Milner, Stephanie Sweitzer, Brian Herman, Carrie Gonell and Jennifer Williams**
(May 11, 2020, 4:38 PM EDT)

Scott Milner

Stephanie Sweitzer

Brian Herman

COVID-19 has caused employers to rethink workplaces. Rapid transformation in the way work is and will be performed, with a majority of the workforce now working remotely, presents a myriad of governance and compliance issues.

As employers embrace this change, they should consider whether information governance and related employment and discovery compliance practices should be adapted to address this new reality.

Information Governance and Maintaining Confidentiality

As more employees work remotely, one key issue is preserving company confidences and data privacy rights during this pandemic. Some considerations for how employers address these issues might include:

- Reminding employees to turn off voice-activated virtual assistants;
- Requesting that employees log out of social media sites while working;
- Instructing employees to maintain a safe work area where household members or roommates cannot view the company's private records;
- Asking employees to use secure messaging platforms;
- Reminding employees not to use personal text or chat messaging platforms for work-related purposes;
- Reminding employees about appropriate storage of business records;
- Confirming records are not being stored outside the corporate environment in unapproved document sharing sites;
- Instructing employees to secure paper documents when not being used and to shred the documents when no longer needed;

- Reminding employees not to dispose of confidential materials in regular waste or recycling
- channels; and
- Reminding employees to secure company hardware and log off while not in use.

Carrie Gonell

Jennifer Williams

Why are these issues important? With employees potentially facing connectivity issues, some may turn to unapproved sites or applications to get business done. When company conference lines are full, employees may look to unapproved alternatives that could create confidentiality issues.

Similarly, employees wishing to collaborate in a less formal fashion may turn to spontaneous social networking applications to rapidly share ideas through voice or video chat rooms. Such applications could lead to information governance and compliance issues. To get ahead of these issues, companies may choose to reconsider their governance policies to address this new reality.

Access to personal data in the company's possession can create additional concerns when employees work remotely. While many companies require the use of virtual private networks to help ensure confidentiality, additional guidance may be considered. This is particularly important in heavily regulated industries.

Regulated health care and life sciences businesses may see regulatory changes designed to assist with information governance. For example, although many tools available to health care and life sciences businesses pre-COVID-19 may not have complied with the Health Insurance Portability and Accountability Act or the EU's General Data Protection Regulation, businesses might reconsider the suspension of various privacy rules, such as the telehealth rules in the U.S. and certain aspects of the GDPR in the EU, to address the public interest in the area of public health.[1]

Information Governance and Employment Issues

Remote work also can create a host of employment issues that dovetail with information governance.

For example, employees might be working at different times or for different durations than anticipated. Companies must keep accurate records of time worked by nonexempt employees, calculate wages correctly, and provide meal and rest breaks to remote employees in those states that require them.[2] To address these issues, employers may consider:

- Setting expectations regarding remote work hours;
- Implementing technological solutions to support nonexempt employees in accurately reporting all of the time they work remotely;
- Reminding management to limit the use of text messaging or communications during off hours; and

- Instructing nonexempt employees who do text or email during off hours that they must record all of their time.

Employers may face further challenges with information governance and data loss if they furlough or lay off workers. Swift action may be necessary to prevent potential data theft or alteration by remote employees impacted by furloughs or layoffs. When conducting large furloughs or layoffs, employers might consider whether to update exit procedures to address preservation of company information in the hands of such employees.

Information Governance and Preservation

The remote workforce also further complicates traditional discovery.

Aside from the routine litigation companies already face, many new litigations are likely to arise as a result of the pandemic — including those for breach of contract; material change in circumstances; frustration of purpose; delay; business impossibility; business losses; supply chain issues; impracticability; force majeure; insurance claims; wage and hour claims; alleged wrongful termination following layoffs; claims of hazardous work environments; and even infringement claims for unauthorized use of products resulting from companies switching operations to assist in the pandemic response.

Because parties must preserve information whenever litigation is or should be reasonably anticipated, both those businesses contemplating litigation and those businesses facing new threats of litigation or actual lawsuits during this time must still preserve relevant, unique information.

To address this preservation obligation, companies might consider:

- Updating legal hold templates to address the new reality e.g., reminding employees not to use devices or sources that aren't supported by information technology to create or store records subject to a legal hold;

- Providing guidance on how to preserve or who to contact should employees use non-IT-supported devices or sources to create or store records subject to a legal hold;

- Updating processes to ensure preservation no matter where relevant information is located, including locations that may not be company-approved but are more likely to be used, such as personal mobile devices, personal computers, personal email accounts, third-party texting applications (e.g., WhatsApp, Viber, Snapchat), third-party document sharing sites (e.g., GoogleDocs, DropBox), and spontaneous social networking applications;

- Sending updated legal hold instructions and reminders to custodians and stakeholders already on legal hold to ensure new material generated during stay-at-home orders is preserved regardless of where it is created or stored; and

- Revising custodian questionnaires and interview scripts to address potential new data sources.

In addition, those already in the midst of discovery will likely face unique collection challenges. Collections may take longer or even be impossible during stay-at-home orders.

Remote collection capabilities will likely be hampered by slow home internet speeds, and for those companies without remote collection capabilities, electronic collections may require the use of remote collection kits sent to an employee's home. Some electronic sources that do not allow for remote access may be unavailable. Similarly, custodians may be unable to access paper files that exist because the files are located in the company office.

Unique data sources created during the stay-at-home orders may further complicate collections. Companies may need to collect mobile devices, messaging applications, social network information and information from document sharing sites — locations from which companies may not be accustomed to collecting.

Collection of such information may raise privacy concerns from employees. Some employees may seek assurances of how the company will maintain confidentiality, while others may refuse to cooperate altogether. Even if the employee provides access to personal devices or locations, there could be additional data privacy implications with personal collections, including access to an employee's financial, health or other personal information.

Working cooperatively with the other side is more important than ever, as strained resources impact discovery. Increased complexity and burdens associated with remote collections should lead to parties negotiating narrowed and tiered discovery.

Failure to implement narrow discovery may lead to an increase in discovery extensions and undue burden objections, with discovery respondents providing information regarding the increased time, costs and burdens associated with responding to discovery in today's remote environment. Meanwhile, courts likely are to look even less favorably on discovery disputes than they already do.[3]

In the long run, discovery proponents may seek discovery of outlier data created during this time. Discovery respondents should be prepared to address issues related to the adequacy of discovery processes during the stay-at-home orders. In the future, deposition topics on preservation and collection may focus on the implementation of legal holds and data creation during the stay-at-home orders.

The bottom line is that evolution in business is creating unique information governance opportunities. As businesses change the way they deliver goods and services to meet market demands, these changes will likely impact information governance.

Companies may continue to leverage remote workforces and employees may continue to work and communicate differently even after the COVID-19 crisis ends. Ultimately, companies should consider how to address remote technologies to maintain confidentiality and privacy, address remote employment issues, and prepare for the creation of new data sources.

Scott Milner is a partner and co-leader of the eData practice at Morgan Lewis & Bockius LLP.

Stephanie Sweitzer is a partner at the firm.

Brian Herman is a partner at the firm.

Carrie Gonell is a partner at the firm.

Jennifer Mott Williams is of counsel at the firm.

[1] See e.g., https://www.morganlewis.com/pubs/the-edata-guide-to-gdpr-coronavirus-v-gdpr-suspending-data-privacy-protection-during-civil-crisis.

[2] See e.g, https://www.morganlewis.com/events/remote-working-in-a-time-of-pandemic.

[3] See e.g., C.W. v. NCL (Bahamas) Ltd., 19-CV-24441 (S.D. Fla. Mar. 21, 2020) (noting how routine discovery disputes are "hardly critical"); Martinez v. Cherry Bekaert, LLP, 18-CV-25429 (S.D. Fla. Mar. 25, 2020) (discussing failure to agree to extensions and how opponent to extension must "provide a comprehensive and rational explanation").