THE JOURNAL RECORD

Gavel to Gavel: Employee privacy and COVID-19

By: Tom C. Vincent II and Joya C. Rutland Guest Columnists March 31, 2021

Tom C. Vincent II

Joya C. Rutland

After more than a year of responding to COVID-19, many companies continue to encounter a range of data privacy issues. At a minimum, the Americans with Disabilities Act, state and local privacy legislation, and state common law govern how employers should be handling sensitive information. Additionally, many companies have self-certified under the EU – U.S. Privacy Shield or have made additional contractual commitments to privacy regarding how sensitive health data is collected, how much info can be disclosed to health officials and employees about positive results, how long they should keep this information, and to what extent this data can be anonymized and retained.

The common approach used for collecting COVID-19 data, under which companies screen individuals but don't retain detailed results, poses a level of risk generally acceptable for most companies due to the generally anonymous and temporary nature of the information obtained. However, tracking whether employees and visitors are vaccinated or requiring the vaccine for entry will require a more personalized inquiry that carries additional legal risks. Therefore, it's important for companies to think about treating such health checks and virus tracking data differently than their typical human resources data – like background checks and benefits information, which are typically put in a personnel file and become subject to lengthy data retention requirements.

In general, employers need a specific reason identified by law as sufficient for collecting health-related information of the nature necessary to implement a workplace COVID-19 response plan. Most applicable laws, such as the ADA, contain relevant exemptions that permit inquiries and data collection that would otherwise be prohibited, and particular agencies (such as the Equal Employment Opportunity Commission) have issued similar guidance. Beyond these permissions, however, an employer must be transparent to its employees if it decides to record vaccination data. Employees must understand why the information is needed; what it will be used for; how it will be kept secure; who will have access to it; and how long it will be kept. This notification could be by way of an updated privacy notice or separate communication.

Tom C. Vincent II and Joya C. Rutland are attorneys with GableGotwals.