Employer Use of Contact Tracing Apps: The Good, the Bad, and the Regulatory

Article By

Taylor Eric White
Carrie Hoffman
John L Litchfield

Foley & Lardner LLP
Coronavirus Resource Center

Related Practices & Jurisdictions

- Communications, Media & Internet
- Consumer Protection
- Coronavirus News
- Labor & Employment
- All Federal

Tuesday, July 7, 2020

Employers struggle with COVID-19 for any number of reasons. However, perhaps one of the main challenges they face is how to keep employees safe, even when one of them tests positive for or is exposed to COVID-19. They are looking for innovative ways to stay a step ahead of the curve. One of the innovations employers are currently considering are contact tracing apps.

In general, a contact tracing app is downloaded to a Bluetooth/Wi-Fi enabled device and allows users to be aware of potential exposure to COVID-19 and enable them to
self-quarantine for the incubation period or seek medical diagnosis. Is an employer’s implementation of a contact tracing app in the workplace a good or bad idea? Are there any legal requirements in play one way or the other? This post will discuss some of the various considerations employers should remember.

At the end of the day, employers may decide to utilize contact tracing apps to augment their own safety protocols and procedures to maintain a healthy work environment amidst the pandemic. However, it is important to remember that there are risks and limitations associated with the use of these apps.

The Good

First things first. There are currently no specific federal- or state-level laws specifically prohibiting employers’ use of contact tracing apps. As the EEOC has noted, COVID-19 constitutes a direct threat under the ADA, so employers may make more robust medical inquiries than would normally be allowed. Certain state-level laws might impact employers’ use of the apps, though, such as California’s general prohibition of electronic tracking devices, requirement that employers reimburse employees for “necessary expenditures and losses,” and prohibition of employer requests for access to personal social media accounts of employees. State-level laws are varied and, of course, rapidly developing, so employers are well-served to monitor relevant jurisdictions closely and consult with their legal counsel before requiring employees to use contract-tracing technology. Generally, however, employers in the United States are, as of this post, permitted to use these sorts of apps, provided they follow various rules and best practices to manage the associated risks—namely, privacy risks.

With that in mind, why would an employer want to take the risks associated with contact tracing apps?

Simply put, employers are struggling to find an efficient path to protect employees, while remaining open for business. Employers are generally required, under OSHA’s General Duty Clause, to provide workers a work environment “free from recognized hazards that are causing or are likely to cause death or serious physical harm.” OSHA has expressed that COVID-19 fits this bill, such that employers must affirmatively act to reduce and manage COVID-19-related hazards in the workplace. As we’ve reported previously, OSHA suggests employers implement some combination of (among other things) personal protective equipment (PPE), cloth face coverings (which OSHA is clear are not PPE), administrative controls, and engineering controls, depending on the level of employee exposure risk involved. Local public health authorities may also impose an added layer of workplace precautions and protections.

In light of this guidance, perhaps one of the most persuasive reasons to utilize contact tracing apps to reduce and manage COVID-19-related hazards in the workplace is in the arguably flexible and efficient technology itself. After installation on a Bluetooth and/or WiFi enabled device, contact tracing apps transmit (usually) anonymous user identification numbers to other app-installed devices within range using the devices’ Bluetooth or WiFi features. If a user reports a positive COVID-19 test, the technology alerts other app users who received the
identification number of the positive user due to proximity. Some apps may have a geolocation feature that creates maps of impacted areas or otherwise only tracks contacts within a particular geographic location (e.g., a workplace). That said, Google and Apple do not use location tracking in their joint Exposure Notifications System (which allows contact tracing apps to notify users who have likely been exposed to COVID-19). Certainly, the apps may have other features that employers may want as well, such as pre-shift COVID-19 symptom reporting.

For these reasons, contact tracing apps may provide a flexible and efficient method to augment employers’ current workplace safety protocols. Use of the apps and an exposure notifications system would, arguably, be quicker and more efficient than traditional contact tracing investigations at identifying exposed individuals in the workplace and isolating them before they can infect others. In this way, employers hope to reduce, or even avoid, the COVID-19 curve in their workplaces.

The Bad

As with any enhancement tied to technology, there are risks and limitations. Further, just as the technology itself provides the most persuasive reason to implement the use of the apps, it also ironically supplies the biggest limitation. That is, the reliability and accuracy of the technology is only as good as its user.

Consider the reality of the modern workplace, be it a factory, office, or other setting, as well as the modern employee in any of those settings. Employees may choose (or be required) to leave phones in their lockers or private workspaces before going to the factory floor, production yard, or conference room. Employees may choose (or be required) to turn their phones off during meetings, or may experience weak WiFi or cellular signals in some workplaces. Or they may forget to charge their phones or even lend them to colleagues or family members. Employees may also be lax or inaccurate in their own manual input of information pertaining to exposure and/or positive COVID-19 tests. In any of these instances, the employees’ actual exposure and contacts (or lack thereof) would not be accurately and reliably recorded in the app.

The obvious risk with this is the potentially dangerous false sense of security the apps could inadvertently provide where all of an infected employee’s actual contacts are not notified of exposure—or conversely, the false alarm and unnecessary business disruption they could create, if someone is notified of exposure when not really exposed. Keep in mind that most of the apps in the marketplace and being developed would create random identification numbers for users, so there is no reliable way to verify accuracy without an independent investigation. Regardless, employers would generally be relying on employees truthful uploading of information about testing positive.

Of course, verification of reliability and accuracy is only part of the risk. Privacy is, frankly, the bigger consideration.

It is worth mentioning that employers often ask about HIPAA when they consider employee medical information. But, in reality, HIPAA only applies to “Covered Entities” (i.e., health plan, health care clearinghouse, or health care provider transmitting health information in electronic form with a covered transaction) and
“Business Associates” (i.e., health information organization transmitting PHI to covered entities; person offering personal health records to individuals on behalf of a covered entity; or a subcontractor creating, receiving, maintaining, or transmitting PHI on behalf of another Business Associate). Most employers would not fit the definitions of either of these phrases.

Nevertheless, the EEOC has cautioned that, while employers may ask employees about whether they are experiencing COVID-19 symptoms and take employee temperatures upon entering the workplace, they must maintain the confidentiality of any information collected regarding employee illnesses and keep any related records for certain periods of time. In the employment context, this means keeping the medical records and information separately from other personnel records and information and limiting access to the same.

In addition to federal EEOC guidance, certain states may have applicable privacy laws as well. For example, California has the Consumer Privacy Act (CPA), for which the California Attorney General just submitted final proposed regulations on June 1, 2020. Under California’s CPA, consumers have various rights pertaining to personal information collected by a business, including a right to disclosure of the information to be collected, deletion (upon request) of the information collected, and to be free from discrimination for exercising these rights. Similarly, the Illinois Biometric Information Protection Act (BIPA) may impose notice and record retention obligations on employees or the app developers themselves. Employers with employees in these and other states with similar laws should therefore ensure these rights are communicated to and permitted to be exercised by employees. Employers should consult their own legal counsel prior to endorsing contract-tracing app use and seek to work with the app developer, where possible, to ensure laws like these are accounted for in the app technology through disclosures, disclaimers, acknowledgments, and consents.

Lastly, and relatedly, a lot of individuals, companies, and governments are racing to develop contact tracing apps. So, employers may have to make a difficult decision on which app by which developer is most appropriate. With this decision comes the consideration of the risk of choosing incorrectly and inadvertently opening employee information to data mining or scams.

The Regulatory

In light of these risks and the current lack of federal law pertaining to the apps, there is some effort in Congress to manage the use. In early June, several Senators introduced a bipartisan bill, called the Exposure Notification Privacy Act, that would regulate the use of contact tracing apps. Among other things, the bill makes participation in the exposure notification systems voluntary, limits the categories of information collected, limits the use of the same, and contains various enforcement provisions. The full text of the bill can be viewed here, and a one-pager summarizing the bill can be viewed here.

Other partisan groups of Senators have introduced related legislation as well, including the COVID-19 Consumer Protection Act (Republican) and the Public Health Emergency Privacy Act (Democrat). There are significant differences between the
three bills in terms of consent, use, and enforcement, and the bipartisan Exposure Notification Privacy Act is certainly narrower in its approach to these issues. However, it is currently unclear how or whether those differences will be resolved. Employers should therefore monitor this sort of federal legislation in addition to staying on top of local and state requirements as well.

For its part, the CDC has published some general guidance on digital contact tracing tools. The CDC suggests that the tools should, among other things, ensure data is secure and confidential, be able to receive input from public health authorities, facilitate identification of known contacts, and be able to send notifications of exposure in multiple electronic formats. While these guidelines currently appear to be geared towards use of digital tools by public health departments, the tenets outlined are worth noting and considering because they are generally consistent with best practices for employers using the apps.

**Conclusion**

In light of the above considerations, if an employer implements a contact tracing app in the workplace, the employer should do at least the following:

- Research which app is most appropriate for the particular workplace at issue; how it works, including how it protects user data; and the background and credentials of the app developer itself.

- Consult legal counsel prior to endorsing a particular app for employee use to appropriately consider privacy, regulatory and other concerns related to contract tracing generally and the terms of use of a particular app specifically.

- Deploy traditional methods to verify the underlying facts pertaining to the employee’s workplace contacts and act accordingly.

- Develop written policies in compliance with applicable laws, informing employees, among other things, how the app works; how it is to be used; what information it collects and provides; and what reimbursement, if any, will be provided.

- Provide training to employees on using the app.

- Obtain signed consents and acknowledgments about use of the app and of the information collected in compliance with any applicable laws.

- Develop and implement appropriate policies and protocols for using and protecting employee information collected through the app.

- Monitor local, state, and federal government agencies and bodies for new guidance and laws pertaining to employee privacy and use of the apps.

In this way, employers will be best suited to manage the various risks associated with the use of contact tracing apps.

© 2021 Foley & Lardner LLP