Since the outset of the COVID-19 pandemic, employers have been engaged in varying levels of contact tracing within the workplace. Contact tracing involves identifying individuals who may have been in close contact with a person who tested positive for the coronavirus while that person was likely infectious. As part of employers’ pandemic response practices, many are implementing policies and procedures that attempt to ascertain the identities of employees who may have been in “close contact” with employees diagnosed with COVID-19, or those suspected of having contracted the virus.

Traditional contact tracing is labor intensive, typically requiring interviews with coronavirus-positive individuals to determine their movements. In some instances, those interviews may extend to family members or others who may be able to provide more information. Given the challenges of conducting contact tracing on a large
scale, as well as the fallibility of human memory relied upon in traditional contact tracing, technology companies are developing digital equipment to aid in the process. Some of the tools are being developed for governmental organizations (indeed, some countries, such as Singapore, have already urged citizens to use contact-tracing digital tools as part of their COVID-19 mitigation efforts), while others are being developed for use by employers within the private sector. Digital contact-tracing tools can assist both with identifying contacts and, potentially, with notification of potential exposure.

**How Does Digital Contact Tracing Work?**

The technology regarding contact-tracing tools is evolving rapidly. Very broadly, digital contact-tracing relies on either one or both of two forms of underlying technology: (1) GPS or cellular location data and/or (2) Bluetooth. The digital contact tracing is typically in the form of an application—or “app”—that alerts the user if he or she has been in contact with someone who has reported having a coronavirus-positive test result or COVID-19 diagnosis, with notification occurring under certain defined parameters (for example, length of time of the contact or proximity of contact). Some apps are tied to smartphones, while others involve wearable smart devices. Similar technology may also be used to help encourage social distancing through proximity tracking and beaconing between devices.

Taking Bluetooth-based, contact-tracing as an example, a broad description of how the technology works is as follows: an app broadcasts unique identifiers over Bluetooth to nearby users of the app. When two users of the app come near each other, the app can estimate the distance between them by measuring Bluetooth signal strength. If, for example, the users are less than approximately six feet apart for a sufficient period of time, the app logs the encounter. When a user of the app identifies himself or herself as having tested positive for a current coronavirus infection or having received a COVID-19 diagnosis, any other user that had an “encounter” can then be notified of the potential infection risk.

The details of how these apps work vary widely and often depend on the technology’s developer. For example, among other details, the following can all vary: what qualifies as an “encounter” (i.e., what is considered an epidemiologically relevant distance and an epidemiologically relevant time period); the details of the notification of infection risks; additional information that may be logged by the app; the hosts of information collected about the app’s users; and the amount of information stored by the app and for how long.

**Official Guidance on Digital Contact-Tracing Tools**

On the federal level, a key component of the White House’s “Opening Up America Again” guidelines are certain “core state preparedness responsibilities” that each state should be able to meet before lifting COVID-19 restrictions. One such responsibility is that states should demonstrate competent ability to conduct certain testing and contact-tracing activities. As relevant to employers, the White House guidance states that employers should “[d]evelop and implement policies and procedures for workforce contact tracing following employee COVID+ test [results].” States and employers that are following the White House guidance are preparing
ways to effectively trace contacts with infected individuals as part of the overall strategy for allowing businesses to reopen to normal operations and, in doing so, return workers to the workplace.

On April 23, 2020, the U.S. Centers for Disease Control and Prevention (CDC) published new guidance and resources for contact tracing, including a “COVID-19 Contact Tracing Training Guidance and Resources” plan, a booklet on the principles of contact tracing tools, as well as a fact sheet discussing some of those digital contact-tracing tools. These materials appear to signal the CDC’s anticipation of a pending surge in contact-tracing efforts around the country as state and local jurisdictions begin to ease COVID-19 restrictions and stay-at-home orders. These new CDC materials are not designed to train, equip, or guide employers in the task of contact tracing. Rather, the plan and related materials are designed for public health authorities to train “[c]ommunity health workers or volunteers with little or no experience conducting contact tracing.” However, the materials offer insight on the type of contact-tracing activities likely forthcoming in states and the types of contact-tracing tasks employers might be expected to perform in conjunction with public health authorities in the event of future workplace exposures.

Additionally, on April 16, 2020, the European Commission issued its “Guidance on Apps supporting the fight Against COVID 19 pandemic in relation to data protection” “to ensure a coherent approach across the EU [European Union] and provide guidance to Member States and app developers” relating to “features and requirements which [contact tracing] apps should meet to ensure compliance with EU privacy and personal data protection legislation, in particular the General Data Protection Regulation (GDPR) and the ePrivacy Directive.” While the guidance is not mandatory, it identifies useful, guiding principles such as:

- the installation of the app on a device should be voluntary and there should be no negative consequences for individuals who chose not to use the app;
- different app functionalities should not be bundled so that an individual can provide his/her consent to each functionality separately;
- if proximity data is used, such data should be stored on an individual’s device (referred to by the Commission as “decentralized processing”). If the data is shared with a health authority, it should be shared only after a confirmation that the user is infected with COVID-19, and only if the user consents to sharing the data;
- the app should be automatically deactivated when the pandemic is declared under control—deactivation should not depend on de-installation by the user;
- the Commission suggests that for determining proximity and close contacts, Bluetooth data is more advisable than GPS or cellular location data as location information “is not necessary for the purpose of contact tracing functionalities”;
- the Commission also recommends that storing the exact time or place of the contact “does not appear necessary,” but that the date of the contact is relevant; and
• the Commission advises that proximity data be deleted as soon as no longer needed for the purpose of alerting individuals, which the EU identifies as a “maximum [of] one month (incubation period plus margin)” or after someone is tested and the result is negative.

The Commission said that the European Data Protection Board will publish further guidance on geolocation and other tracing tools in the context of COVID-19.

**Key United States Labor and Employment Considerations**

There are many unanswered questions about how contact-tracing apps will work and how effective the tools will be. Employers evaluating these tools may want to review carefully any tool and its functionality before implementing a contact-tracing app in their workplaces. Among other issues, it is important that employers evaluate and understand technical issues including, but not limited to, the following:

- what data is being collected;
- how the data is being stored (on an individual’s device or an external server);
- how long the data will be kept/stored;
- whether the app’s developer has continued access to the information; and
- what data security measures are in place (such as encryption and anonymization).

Employers may also want to evaluate and decide how contact-tracing tools will be tailored for their workplaces. Factors include, for example:

- will use of the tool be voluntary or mandatory;
- if mandatory, will employees be discharged if they refuse to use the tool or “turn it off”;
- will the tool will only track contacts during work hours or outside work time; and
- who in an organization will have access to information collected through the tool.

These are just a few of the questions that employers may want to answer when vetting tools they are considering deploying in a particular workforce.

Since these tools continue to be developed at a rapid pace, it is likely that additional guidance from federal and state jurisdictions will be issued. For now, as employers look into this rapidly evolving area, it is prudent to evaluate the following labor and employment issues:

**Data and cybersecurity considerations.** Unlike the EU, there is no nationwide data privacy law in the United States. However, various states, such as California, have developed laws relating to data privacy and security that
should be consulted as an employer considers contact-tracing tools. For example, California’s Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, may impose requirements regarding employee notification and other obligations for employers. Further, a number of states (including Illinois and Texas) have adopted biometric privacy laws that, depending on what is collected by the contact-tracing app, could be implicated. Moreover, some contact-tracing tools may collect personal information that is potentially subject to state data breach notification requirements.

- **State law considerations.** When reviewing state law privacy issues, consider and identify strategies to mitigate the risk of common law claims for invasion of privacy relating to contact-tracing tools, particularly if the tools track employees engaged in privacy-sensitive activities such as going to the restroom or a nurse’s office at the workplace. In addition, when reviewing state laws regarding electronic monitoring keep in mind that some states may have specific laws that are implicated by these tools. For example, Connecticut’s Electronic Monitoring Act precludes employers from engaging in any electronic monitoring without first providing prior written notice to all employees of the types of monitoring which may occur.

- **National Labor Relations Act (NLRA) Considerations.** Employers may also want to ensure compliance with the NLRA, which has a well-developed and detailed body of case law regarding employer surveillance activities. Additionally, if a workforce is unionized, employers should consider whether the deployment of contact-tracing apps implicates a duty to bargain with any relevant labor union.

- **Health Insurance Portability and Accountability Act (HIPAA) considerations.** Employers that are considered covered entities under HIPAA may wish to evaluate the extent to which data from the contact-tracing tools may contain information subject to HIPAA’s confidentiality requirements and use restrictions.

- **Employee relations considerations.** General employee relations and equal employment opportunity compliance issues are other important subjects to consider. For example, employers may want to consider strategies to prevent stigmatization of employees who have been diagnosed with COVID-19, or who have close contacts with employees who are COVID-19 positive. Inclusiveness is also critical both from an internal equity perspective as well as from the perspective of the effectiveness of contact-tracing tools, so employers may find it useful to have a plan for managing those employees without smart devices, as well as those who need additional assistance (such as individuals with disabilities) in order to use devices. Moreover, depending on what information is collected through a tool, disability discrimination issues could arise—for example, a contact tracing app could collect information about how often an employee goes to the bathroom, which could lead to assumptions that an individual has a disability.

Proactively identifying these and related compliance issues, as well as developing strategies to avoid or mitigate risk, are prudent steps to take before implementing any contact-tracing tool. Employers may wish to consider developing clear policies,
disseminated to and acknowledged by all employees, that provide notice regarding
the contact-tracing tools to be used and that explain (at a high level) how the tools
work, the rationale for the tools, and other critical information regarding how
employee data will be used and safeguarded. Transparent policies regarding any
contact-tracing tool deployed in a workplace may be a sensible consideration for
some employers both from legal compliance and employee relations perspectives.


Source URL: https://www.natlawreview.com/article/update-coronavirus-contact-tracing-status-benefits-and-key-considerations