August 3, 2020

Protecting Employees From COVID-19 Without Violating Their Privacy Rights

Christian R Everdell; Marvin J Lowenthal

A common response to widespread disease has always been to avoid contact with others until the disease runs its course. Many states adopted that approach to combat the COVID-19 outbreak by implementing stay-at-home orders, social distancing protocols, and other similar restrictions. Businesses responded in kind by encouraging or mandating work-from-home or telework arrangements for their employees. But now that states are reopening after their COVID-19 lockdowns and allowing employees to return to their offices – like New York did on June 22 – employers must implement safety measures to protect their employees.

Despite the pressing need to protect employees' health, employers cannot forget their obligation to protect employees' privacy. This article discusses several of the most common safety measures businesses have been considering implementing to protect their employees during the ongoing COVID-19 pandemic, as well as how various privacy laws may be implicated by these measures. The article concludes by identifying a few general points for employers to consider when developing policies and procedures to protect their employees.

Safety Measures under Consideration

Three of the most common safety measures employers are considering to protect their employees as they return to work are: (1) temperature screening, (2) medical testing, and (3) contact tracing. Each potential safety measure is described below.

1. Temperature Screening

Because fever is one of the most common symptoms of COVID-19,[1] essential businesses that remained open throughout the pandemic have often utilized temperature screenings. A temperature screening involves measuring a person's temperatures before they enter a building or designated location. Anyone whose temperature exceeds a predetermined level will be denied entry or directed to a specified location. Temperature screenings can be conducted using a variety of methods from traditional thermometers to contact-free scanners with facial-recognition technology.

2. Medical Testing

Medical testing can detect whether a person has a current COVID-19 infection ("Viral Test") or antibodies that indicate a past COVID-19 infection ("Antibody Test"). Each of these tests can potentially provide employers with relevant information. A Viral Test is conducted by collecting a sample from a person's

[1] https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus/coronavirus-symptoms-frequently-asked-questions.

oral or nasal surfaces using a swab. A person who tests positive for a current COVID-19 infection may be contagious and therefore poses a potential risk to others. An Antibody Test is conducted by collecting a blood sample. A person who has antibodies against COVID-19 may be less likely to be infected again if exposed to the virus.

3. Contact Tracing

Because the CDC has identified close person-to-person contact as the primary and most important mode of transmission for COVID-19, tracking who an infected person has come into contact with can help contain the spread of the virus. Contact tracing apps generally work by recording who each user comes into contact with and alerting users if they came into contact with someone who was infected with COVID-19 while that person may have been contagious. The alerted people can then quarantine themselves to limit the spread of the virus.

Contact tracing apps ordinarily discuss two general methods for identifying who a user has come into contact with. Some apps plan to monitor users' GPS locations, which would allow the app not only to alert users that they have been exposed to an infected individual but also to collect data on where that interaction occurred. Other apps propose using Bluetooth technology to exchange anonymous keys when users remain within a certain proximity for a certain period of time. There are then two ways to use those anonymized keys. In a centralized process, each user's anonymized key and the anonymized keys of anyone that user came into contact with are uploaded to a central database. When someone is diagnosed with COVID-19, the tracking app checks the database and informs any users who came into contact with that person while he or she was potentially contagious. In a decentralized process, the anonymized keys of each person the user came into contact with remain on the user's phone. When one of the users is diagnosed with COVID-19, the tracking app lets everyone know that that anonymized key was diagnosed with COVID-19, and the app informs anyone with that key on their phone that they have had contact with an infected individual. In sum, a centralized process matches infected users to people they had contact with in a centralized database while a decentralized process conducts that matching on each individual user's phone.

Typically, contract tracing apps contemplate users self-identifying when they are diagnosed with COVID-19. It is possible, however, that some contact tracing apps will interface with a user's medical records so that a positive COVID-19 diagnosis is immediately detected and utilized by the app.

Potential Privacy Implications

Employers conducting even the relatively straightforward safety measures described above place themselves at the crossroads of a variety of privacy regulations. Below we briefly discuss five areas where privacy regulations may significantly impact the procedures employers devise for protecting their employees who return to work during the COVID-19 pandemic.

A. Biometric Data Regulations

Multiple states now have regulations that protect an individual's biometric data. These include the New York Shield Act, which requires businesses to implement reasonable safeguards and imposes breach notification obligations, and Illinois' Biometric Information Privacy Act ("BIPA"), which requires employers and others to obtain informed consent prior to collecting biometric information. Employers would do well to pay particular attention to the BIPA, if applicable, as it includes a private right of action with statutory penalties for violations.

None of the safety measures discussed above necessarily collect biometric data, but employers may implement the above safety measures in a way that captures biometric data. For example, taking someone's temperature alone would generally not be covered by regulations that protect a person's biometric data, but temperature screenings can be performed using facial-recognition technology to create a contact-free screening that automatically tracks the results for each employee, which may be covered.[2]

B. California Consumer Privacy Act ("CCPA")

The CCPA regulates the collection of a California resident's personal information. Personal information includes certain categories of information that "is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[3] In relevant part, those categories include "geolocation data"[4] and "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual" other than information made publicly available from government records.[5] However, the CCPA contains a limited exemption for employee information, allowing employers to avoid many of the CCPA's obligations when implementing safeguards against COVID-19.[6] But employers must still comply with the CCPA's notice provisions (*e.g.* they must inform employees about the categories of personal information to be collected and the purposes for which that information will be used) and its data protection provisions as well.[7]

As described above, the CCPA defines protected personal information broadly. Therefore, the CCPA's scope is likely broad enough to encompass information collected by medical testing and contact tracing apps, and could even potentially capture information from temperature checks depending on what information is recorded in addition to the temperature.

C. Americans with Disabilities Act of 1990 ("ADA")

The ADA requires that any mandatory medical test for employees be "job related and consistent with business necessity." The EEOC has issued guidance explaining that employers may "take steps to determine if employees entering the workplace have COVID-19 because an individual with the virus will pose a direct threat to the health of others. Therefore an employer may choose to administer COVID-19 testing to employees before they enter the workplace to determine if they have the virus."[8] The EEOC has also issued guidance stating that employers may measure employees' body temperature during the pandemic.[9]

---

[2] *See, e.g.*, BIPA, 740 ILCS 14/10 (defining a protected "biometric identifier" to include "scan of hand or face geometry"); N.Y. Shield Act, Gen. Bus. Law § 899-AA(1)(b) (defining "private information" to include personal information paired with biometric information, including "data generated by electronic measurements of an individual's unique physical characteristics . . . which are used to authenticate or ascertain the individual's identity.").
[3] Cal. Civ. Code 1798.140(o)(1).
[4] Cal. Civ. Code 1798.140(o)(1)(G).
[5] Cal. Civ. Code 1798.80(e).
[6] Cal. Civ. Code 1798.145(h)(1)(A) ("This title shall not apply to any of the following: (A) Personal information that is collected by a business about a natural person in the course of the natural person acting as . . . an employee of . . . that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as . . . an employee of . . . that business.").
[7] Cal. Civ. Code 1798.145(3).
[8] https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws ("May an employer administer a COVID-19 test (a test to detect the presence of the COVID-19 virus) before permitting employees to enter the workplace? *(4/23/20)*")
[9] https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act

The above EEOC guidance indicates that employers may require employees to submit to temperature screenings and Viral Tests. The logic of the guidance, however, does not necessarily authorize employers to require employees to submit to Antibody Tests, because Antibody Tests show that a person may not get sick; the test does not identify individuals who pose a direct threat to the health of others. Therefore, employers who plan to require Antibody Tests will need to ensure they can do so compliant with the ADA. In addition, employers need to keep in mind that even though temperature screenings and Viral Tests may be required, the results of those tests may still constitute confidential medical information under the ADA, which can only be disclosed to certain people in limited circumstances.[10]

D. Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

HIPAA safeguards the privacy of protected health information ("PHI"), which is health information that is individually identifiable. HIPAA's restrictions apply only to "covered entities" (i.e. health plans, health care clearinghouses, and health care providers)[11] and their "business associates," which are defined as entities who perform certain activities or services on behalf of a covered entity.[12]

To the extent HIPAA applies, all of the safety measures under consideration are likely to capture protected health information, with the possible exception of a contact tracing app that collects no health information other than voluntary submissions from users who have tested positive for COVID-19. Although HIPAA is unlikely to apply to most employers, it cannot be dismissed out of hand because the term "covered entities" is broader than it appears. For example, employers operating self-funded health plans may themselves be considered a health plan.

E. Information Security Laws

Many states have established laws that require entities that collect personal data to implement reasonable security measures to protect that data and to inform people if their personal data is exposed in a data breach. The data protected by these laws can vary widely. For example, the CCPA's broad scope is described above, but the New York Shield Act generally protects a narrower universe of private information, including social security numbers identification card numbers, account numbers or other identifiers accompanied by information that would allow access to those accounts, and biometric information.

Information that falls within the scope of an applicable information security law must be maintained in accordance with the restrictions that law imposes. Generally, medical testing or collecting data through a contact tracing app will likely create some record that must be considered for potential compliance with information security laws, and temperature screenings may as well unless the employer is simply measuring people at the door with a thermometer without additional record keeping.

Considerations for Employers

In light of the variety of privacy regulations to which employers may be subject, employers should consider a few key points when implementing safety measures to protect employees returning to work during the COVID-19 pandemic:

[10] *Id.*
[11] 45 C.F.R. § 160.103 (defining "covered entity").
[12] 45 C.F.R. § 160.103 (defining "business associate").

1. *Understand How Data Is Collected and Used*

For any safety measures an employer is considering implementing, the employer must understand what data is being collected, how the data will be used and stored, and who can access the data. For example, different regulations may apply depending on whether a temperature check records biometric data. Employers may need to take particular care in understanding the data flow of any contact tracing app, especially if it was developed by a third party.

2. *Determine Whether to Store Data*

An employer may choose to store data demonstrating the implementation of safety measures to protect its employees for many reasons. Some employers will be required to maintain certain data, such as those subject to New York's Office-Based Work Guidelines for Employers and Employees, which require employers to "[r]eview all responses collected by the screening process on a daily basis and maintain a record of such review."[13] Other employers may want to be able to demonstrate that they consistently applied safety measures in case people nonetheless get sick at work.

Various privacy protections may apply to employee data that is created through employer-established safety measures. Employers should therefore be thoughtful about what information they are retaining about employees and why they are retaining it.

3. *The Legal Landscape Changes Rapidly*

Employers are only just beginning wide-spread implementation of safety measures to protect employees from COVID-19. As different employers apply these safety measures in a variety of situations, legal questions and concerns will no doubt arise that were not anticipated at the outset. In addition, legislatures and regulators may impose rules governing the use of certain safety measures. For example, on June 1, Senators Maria Cantwell and Bill Cassidy introduced the Exposure Notification Privacy Act, which seeks to regulate contact tracing apps.

Given how rapidly the applicable laws and regulations may change, employers should work with their compliance teams and legal counsel to implement appropriate safety measure to protect their employees and to ensure those measures remain compliant as the law evolves.

[13] https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/OfficesSummaryGuidelines.pdf

The Authors:

Christian E Everdell
Partner

+1 212 707 7268
ceverdell@cohengresser.com

Marvin J Lowenthal
Associate

+1 212 707 1334
mlowenthal@cohengresser.com

About Cohen & Gresser:

Cohen & Gresser is an international law firm with offices in New York, Seoul, Paris, Washington, DC, and London. We have an outstanding record of success in high-stakes and high-profile litigation, investigations, and transactional work for our clients, including major financial institutions and companies across the world. Our attorneys have superb credentials, and are committed to providing the efficiency and personal service of a boutique law firm along with the quality and attention to detail that are the hallmarks of the best firms in the world. The firm has been recognized in a wide range of publications, including *Chambers* and *The Legal 500*.

New York | Seoul | Paris | Washington DC | London

www.cohengresser.com
info@cohengresser.com
+1 212 957 7600

View C&G's Profile