ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Back to the Office? COVID-19 Screening and Tracking

Employment and Labor

Health Law

Employers and employees are working together to pivot on a moment’s notice to comply with ever-changing guidance from public health authorities at all levels of government.

To try to get the US economy back on track, on April 16, 2020, US President Trump unveiled guidelines for “Opening Up America Again,” which set forth a three-phase approach based on the advice of such public health experts. Dovetailing on these White House guidelines, state governors developed local orders seeking to responsibly open back the economy, instructing employers to take specific actions regarding physical workplace modifications as well as screening protocols in compliance with public health expert COVID-19 requirements.

For example, New York Governor Andrew M. Cuomo issued Executive Order No. 202.38 that allows businesses to require individuals to undergo temperature checks and deny entry to those individuals who refuse or whose temperature is above that prescribed by the New York State Department of Health guidelines.

Formulating a workplace safety strategy

Best practices for employers dictate recognizing that there is no one size fits all strategy; hence, this article’s theme that flexibility and compassion are the cornerstones of success for employers tackling workforce and workplace considerations related to reopening their worksites in COVID-19 times.

To start, employers should review the New York Forward Business Reopening Lookup Tool for and the California Resilience Roadmap. Indeed, the purpose of this article is to discuss different workplace safety practices, such as (internal workplace, see privacy discussion below) digital contact tracing and temperature taking, that employers should evaluate when fashioning a tailored approach to reopening for “in person” business.

The first step is establishing a reopening team that will outline a return to work protocol, and possibly a formal Standard Operating Procedure. For example, employees with HR experience can work with legal counsel and accountants to update employee leave policies and employee handbooks, create a plan for individual requests to continue telecommuting, devise a plan to onboard furloughed employees, and prepare for the impact of reporting compliance for Small Business Association’s Paycheck Protection Plan (with modifications made on June 5, 2020 to the Paycheck Protection Program Flexibility Act of 2020).

This task force should also involve individuals with an interest in keeping up to date on governmental guidance, including:

- Maintaining confidentiality of employee’s medical information acquired during lawful workplace screenings, such as taking temperatures or asking about exposure to COVID-19;
- Adhering to social distance requirements;
- Instituting proper disinfecting of frequently touched surfaces*;
- Conducting a risk assessment and configuring workspaces in compliance with OSHA;
- Maintaining a healthy work environment in compliance with CDC guidelines; and
- Determining whether local laws require employers to provide personal protective equipment.

*Manufacturing company employers who are FDA audited should be mindful of heightened COVID-19 sanitization that may be flagged by FDA upon audit. When opening manufacturing sites, manufacturing site-employers should consider developing updated (CDC guidance-compliant) standards of sanitization, and ensure that completion reports are generated and posted in public areas.

Also, employers must be proactive in advance of reopening by selecting one individual on this

internal team to reach out to third parties that are responsible for maintaining the office space (i.e., landlords or property management companies, cleaning companies) and vendors that provide supplies or services (i.e., technology, mail, copiers, office supplies). Communication from the employer is key to alleviating employee anxiety; hence, there should be regular updates and a designated point person to field any concerns of employees or answer questions seeking clarifications to exceptions to policies and procedures.

At this planning stage, the COVID-19 task force team should assess feasibility of implementing in-company digital contact tracing. Policies and procedures developed for in-company digital contact tracing must be limited to collecting tracing information from employees that advances the organization's vested interest to determine who are well. Those who have a sick family member at home with COVID-19 should notify their supervisor and follow CDC recommended precautions.

Thus, an employee's contacts in the outside world are relevant to an in-company digital contact tracing to the extent that such outside world contact may give rise to an employee's affirmative duty to report such exposure to its employer and to self-isolate under the CDC guidelines.

Additionally, an employer should review the EEOC's Technical Assistance Questions and Answers (updated on June 11, 2020) explaining an employer's responsibilities under the ADA, Rehabilitation Act and EEOC laws related to COVID-19, which discusses the types of screening questions an employer is allowed to ask as to associated symptoms to determine if an employee "poses [a] direct threat to the health in the workplace" and the with whom the infected employee came into contact within the organization (as opposed to the outside world).

The CDC interim guidance to businesses states that "employers should actively encourage sick employees to stay home" and states that: (1) "employees who have symptoms should notify their supervisor and stay home" and (2) "employees circumstances permitting an employer to administer COVID-19 testing under the ADA requirement "that any mandatory medical test of employees be job related and consistent with business necessity."

Another reason that work protocols should expressly communicate to employees such limitation on the collection of digital tracking data by the employer is that a failure to do so by the employer may violate notification and privacy concerns and/or certain state laws already in place. (At the federal level, two bills have been drafted and are both pending legislation before Congress; see below discussion).

Second step, employers should seek legal counsel regarding plans to enforce social distancing by employees at the worksite, policies for interactions with visitors to the worksite, and employee attendance at offsite events. At that time, employers should also discuss whether to allow certain employees to return to work on a rotating basis, especially if the staggering of work hours is necessary to keep the social distance necessary to comply with OSHA or CDC regulations. During such consultation, employers furthermore should seek guidance on any special accommodations that may be necessary to implement for "high-risk" employees.

This social distance component is especially crucial for employers who have offices with many open spaces. In such instances, employers should restrict use of communal spaces by making sure that no employees share phones, desks, or workstations, and that there are assigned time slots for on-site cafeterias.

Similarly, there should be postings limiting the number of employees allowed in elevators, bathrooms,

and other common areas. Moreover, to prevent employees from walking past each other in the hallway, to the extent possibly, employers should create “one way” hallways. These are just a few of the considerations to spur a discussion on best practices by employers as they fashion appropriate policies for returning to work.

Privacy and notice concerns related to digital contact tracing

Yet another consideration is whether in light of technological advances, employers should implement app-based technology to track digital data for public health purposes during the COVID-19 pandemic as part of a worksite safety strategy. Employers reopening for “in person” business should review the Centers for Disease Control and Prevention’s (CDC) useful resources for COVID-19 contact tracing as well as its guidelines for COVID-19 digital contact tracing tools. Specifically, the collaboration between Apple and Google on a contact tracing initiative for “exposure notification” allows smartphones to gather data that can be used to notify individuals that may have been exposed to COVID-19.

Notably, as of August 24, 2020, only eight out of 50 states have agreed to participate in exposure notification, which can be problematic because of the importance of critical mass participation for digital contact tracing to be effective. Perhaps a way to encourage such mass participation is by making the public more aware of the apple-google contact tracing app’s “privacy redaction ability” (a term I coined to explain the app’s feature that allows a user to prevent disclosure of that user’s individual identity by hiding, blurring, or encrypting sensitive location information).

The aforementioned privacy redaction ability is different from the scenario where an employee elects to “opt-out” of participating in an employer’s in-company digital tracking workplace protocol which “opt-out” would warrant the employer’s de-identification of the “opted-out” employee’s personal information.

Against this backdrop, it is important to evaluate the privacy and notice concerns for employers vis-à-vis the COVID-19 Consumer Data Protection Act of 2020 and Public Health Emergency Privacy Act (PHEPA) bills currently before Congress that seek to protect the privacy rights of individuals to such collected digital data. The first bill, the COVID-19 Consumer Data Protection Act of 2020 was introduced in the Senate on May 7, 2020 and co-sponsored by Republican Senators Roger Wicker, John Thune, Jerry Moran, Marsha Blackburn, and Deb Fischer.

Its purpose is “[t]o protect the privacy of consumers' personal health information, proximity data, device data, and geolocation data during the coronavirus public health crisis” by requiring “affirmative express authorization,” but excluding from covered aggregated data, business contact information, de-identified data, employee screening data, and publicly available information.

Note that based on the definition of employee screening data in this bill, employers would be wise to keep contemporaneous records showing compliance that if such digital data was collected it was used to determine whether to permit an individual to enter the employer’s physical site of operation. Also, potential liability to the employer may arise due to this bill broadly defining a covered entity to include one that “collects, processes, or transfers such covered data, or determines the means and purposes for the collection, processing, or transfer of covered data.”

The reason that this bill, the COVID-19 Consumer Data Protection Act of 2020, needs to be on the radar of employers now is because if it becomes law, there are only 14 days after the Act is enacted for employers to prepare a Privacy Policy that fulfills the transparency requirement delineated in

Section 3 entitled Privacy of Covered Data, which in relevant part, provides:

PRIVACY POLICY—A covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall, not later than 14 days after the enactment of this Act, publish a privacy policy that:

- Is disclosed in a clear and conspicuous manner to an individual prior to or at the point of the collection of covered data for such a purpose from the individual;
- Is made available in a clear and conspicuous manner to the public;
- Includes whether, subject to the affirmative express consent requirement of subsection (a), the covered entity transfers covered data for such a purpose and the categories of recipients to whom the covered entity transfers covered data for such purpose;
- Includes a general description of the covered entity's data retention practices for covered data used for a purpose described in subsection (b) and the purposes for such retention; and
- Includes a general description of the covered entity's data security practices.

Additionally, employers should loop in their insurance professionals to determine whether their existing policies adequately protect them because if an employer's implementation of digital contact tracing runs afoul of the strict requirements enunciated in the COVID-19 Consumer Data Protection Act of 2020, employers should be forewarned that Section 4 Enforcement provision of this bill allows the consolidation of actions brought by two or more State Attorneys General or authorized state governmental authority.

The Democratic Senators Richard Blumenthal and Mark Warner, in response to the COVID-19 Consumer Protection Act of 2020, on May 14, 2020 introduced the second bill entitled the Public Health Emergency Privacy Act (PHEPA). The purpose of the PHEPA bill is similar; to wit "[t]o protect the privacy of health information during a national health emergency." As with the COVID-19 Consumer Protection Act of 2020, there are several best practice concerns for employers throughout this bill.

First, will the employer be considered an excluded covered organization that would require proving that the employer is engaged in a "de minimis collection or processing of emergency health data"? Second, does it make economic sense for employers to invest in digital contact tracing given the many affirmative duties discussed in Section 3 "Protecting the Privacy and Security of Emergency Health Data" of this bill?

For example, employers that do not fall within excluded covered organizations would be required to:

1. Provide an effective mechanism to assure the accuracy of data being collected and allow an individual to correct inaccurate information;
2. Provide safeguards to "adopt reasonable safeguards to prevent unlawful discrimination on the basis of emergency health data";
3. Have a mechanism in place to allow an individual to revoke consent and within 15 days of said revocation stop collecting such data;
4. Provide an individual privacy policy that complies with notice requirements delineated in the bill; and
5. Potentially have to keep the data for a significant amount of time depending on when public health emergency is terminated. Third, can an employer afford appropriate insurance coverage to be able to defend itself against private causes of actions?

The bill explains:

> (A) IN GENERAL—Any individual alleging a violation of this Act may bring a civil action in any court of competent jurisdiction, State or Federal.
>
> (B) RELIEF—In a civil action brought under paragraph (1) in which the plaintiff prevails, the court may award — **(i) an amount not less than US$100 and not greater than US$1,000 per violation against any person who negligently violates a provision of this Act; (ii) an amount not less than US$500 and not greater than US$5,000 per violation against any person who recklessly, will fully, or intentionally violates a provision of this Act; (iii) reasonable attorney's fees and litigation costs; and (iv) any other relief, including equitable or declaratory relief, that the court determines appropriate.** (Emphasis added.)

Creating safe worksites as the economy reopens during COVID-19 requires employers to develop best practices that safeguard the privacy interests of individuals, who consent to participate in digital contact tracing. In evaluating whether to implement digital contact tracing, employers must also determine the risk of exposure to third parties if a visitor or employee opts to not participate in the first place, chooses to thereafter withdraw consent and stop participating or decides to blur or redact locations.

Conclusion

Even the best laid plans must adapt to change. Given the current COVID-19 legal and medical landscape, employers that seek to maintain an engaged workforce must review their protocols and procedures on a regular basis and perhaps weekly to abide by the changing government guidelines.

Jennifer F. Nelson

Partner and Group Head of Virtual-Fractional General Counsel Practice Group

Jennifer N. Flynn is partner and group head of Dorf Nelson & Zauderer LLP's Virtual-Fractional General Counsel Practice Group, where she provides virtual and fractional general counsel, deputy general counsel, and chief privacy officer services to small to mid-size businesses to meet their in-house legal needs.

Prior to her current position, she served as president, chief legal officer, and chief operating officer for an artificial intelligence tech startup, where she sat on the board of directors.

She has also served as vice president, deputy general counsel, chief privacy officer, and assistant corporate secretary for two CPG public companies, Prestige Consumer Healthcare Inc. and Zevia PBC.

Adriana E. Kierszenbaum

Counsel

Dorf & Nelson LLP