Session CLE 504 | Privacy During a Pandemic: The New Reality of Staying Safe, Healthy and Employed

Technology is a key component to controlling the spread of COVID-19 and reopening the economy. Widespread testing, fever detection technology, and antibody certificates may be reasonable and necessary, but what about AI surveillance and tracking using geolocation and biometric facial recognition technology? Should governments, businesses and employers be permitted to monitor their citizens, customers and employees in order for people to leave their homes, shop in grocery stores or return to work? Are these practices lawful, ethical or justified during a state of emergency? Are these intrusions into individual privacy rights temporary? What does “data privacy” entail in this new reality? Join privacy, technology, civil liberties and employment law experts for an interactive discussion on privacy in the time of coronavirus and what we are willing to give up to stay safe, healthy and employed. The attendees will gain an understanding of the use of technology to control the spread of the novel coronavirus and its impact on individuals' data privacy, civil liberties, and employment rights. The attendees may voice their concerns and opinions, hear differing and opposing points of view and walk away with a new perspective on privacy implications when advising clients on the technology or policies they may be considering or implementing in their businesses.

Moderator:
Grace Wen, Counsel, Binder & Schwartz LLP

Speakers:
Dorit Rubinstein Reiss, Professor of Law and the James Edgar Hervey ‘50 Chair of Litigation, University of California, Hastings College of the Law
Devjani H. Mishra, Shareholder, Littler Mendelson PC
Neyha Rajan, Assistant General Counsel, Tailor Brands, Inc.
Jennifer Lee, Technology & Liberty Project Manager, ACLU of Washington
PRIVACY DURING A PANDEMIC
THE NEW REALITY OF STAYING SAFE, HEALTHY AND EMPLOYED
Government, Public Health & Safety v. Individual Freedoms, Civil Rights & Privacy

- Technology Assisted Contact Tracing (“TACT”) or exposure warnings—effectiveness and limitations of geolocation applications (proximity tracking and/or heat maps), use of AI
- Quarantine and/or mask/face covering violations – fines
- Surveillance, temporary limits on travel, right to congregate—Lessons from the Past, e.g., 9/11 and HIV epidemic, disproportionately impacted communities; border protection
- Legislative proposals—“Public Health Emergency Privacy Act” and Exposure Notification Privacy Act
Employer Responsibilities & Obligations v. Employee Privacy

• Temperature & health screenings—compliance with HIPAA, OSHA, ADA and other labor laws
• Antibody testing—EEOC Guidance
• Mandatory vaccine when available?
• Legislative proposal—states prohibiting employers from requiring location tracking applications
• Residential privacy arising out of working remotely
Business Needs v. Consumer Privacy

• Mask and face coverings
• Fever detection technology including thermal cameras, kiosks and other devices embedded with facial recognition capabilities
• Notice and consent for collection and processing, data retention and disposal & sharing data with government
• CCPA (and other consumer privacy regulations) and Biometric Privacy laws – Enforcement has not slowed
• Legislative proposal—COVID-19 Consumer Data Protection Act
Contact Tracing Technology

- How should the public’s ‘need to know’ their exposure to past and current infected individuals be weighed against an individual’s interest in maintaining personal privacy about their own health conditions?

- According to the CDC, digital contact-tracing tools can add value to traditional contact tracing by:
  - improving the efficiency and accuracy of data management and automating tasks,
  - reducing the burden on public health staff by allowing electronic self-reporting by patients and contacts, and
  - using location data, such as Bluetooth or GPS, to identify community contacts otherwise unknown to the case to review possible exposure.

- Users of such reporting systems elect to share data and are alerted if they have been close to a COVID-19 patient.
Use Of Apps In The Covid-19 Response And The Loss Of Privacy Protection

- Nature Medicine conducted an analysis of 50 COVID-19-related apps, including their use and access to personally identifiable information, to ensure that the right to privacy and civil liberties are protected.

- The most common functionalities include live maps and updates of confirmed cases, real-time location-based alerts, systems for monitoring and controlling home isolation and quarantine, direct reporting to government, self-reporting of symptoms and education about COVID-19.

- Of the 50 apps analyzed in the nature medicine study, 30 required permission for access to the user’s mobile device. Some of the apps explicitly state that they will use "information about the person’s age, email address, phone number and postal code; the device’s location, unique device identifiers, mobile IP address and operating system; and the types of browsers used on the mobile device." Others "demand access to contacts, photos, media, files, location data, the camera, the device ID, call information, the wifi connection, the microphone, full network access, the google service configuration, and the ability to change network connectivity and audio settings."

- Despite all of the data being used and collected, the study found that only 16 of the 50 apps analyzed stated that users’ data would be made "anonymous, encrypted and secured and will be transmitted online and reported only in an aggregated format."

Report available here: [HTTPS://RDCU.BE/B7EVL](HTTPS://RDCU.BE/B7EVL)
Problems With Other Tracing Technologies

• Remote or Standoff Fever Detection ("Thermometer Guns")
  • Elevated body temperature can be caused by many factors other than COVID-19.
  • COVID-19 is contagious well before symptoms appear, and many infected people never develop any symptoms, including fever.
  • Standoff fever detectors are far less accurate than traditional internal thermometers.

• Thermal Cameras ("Fever Detectors")
  • Only to be used to measure one subject at a time and in conjunction with a more accurate backup means of measuring temperature;
  • Environmental and system setup factors can influence accuracy, such as screening background, ambient temperature, cameral location and positioning.

• Drone Thermal Scanners
  • Drones have been sighted flying over parks to look for social distancing violations (how can it know which people are members of the same household?) and shout admonishments at those who appear to be in violation, for example.
  • The use by police of these loud, short-battery life devices — which are not permitted by the FAA to be flown over people or beyond the line of sight of the operator — is more likely to acclimate people to drone surveillance than it is to slow COVID.
Privacy Issues With Fever Detectors

- While a voluntary remote temperature check is not a serious invasion of privacy, especially if individual records are not retained, it is not something we would want companies or government agencies to routine collect.

- This crisis threatens to normalize such biometric surveillance, with the result that even after a vaccine is distributed and COVID-19 retreats as a public health threat, new infrastructures for the routine and unquestioned collection of such data will remain.

- Thermal cameras were previously used to detect concealed guns before the outbreak and were repurposed for temperature checks. But it’s not hard to imagine a network of thermal cameras created to fight the coronavirus repurposed for these suspicionless thermal body searches.

- Most importantly, any use of tracking apps is voluntary. Users may choose to share their information, or not, which inherently limits the efficacy of any contract-tracing application.
Vaccines

Vaccine requirements are not uncommon

• In the united states, most vaccine mandates come from the government. The advisory committee on immunization practices (ACIP) makes recommendations for both pediatric and adult vaccines, and state legislatures or city councils determine whether to issue mandates.

• These mandates are most commonly tied to public school attendance, and all 50 states require students to receive some vaccines, with exemptions for medical, religious, and philosophical reasons.

Should employers require workers to take vaccines?

• Legally, employers can make it mandatory

• Requiring it may be counterproductive

Alternatives to mandates -- Instead of requiring vaccination as a condition of employment, employers could:

• Require it to work from the office.

• Legally, employers would be required to make reasonable accommodations for workers who refuse to get vaccinated. Such an accommodation could include allowing them to work from home, which millions of Americans are already doing.

• Advocate voluntary inoculation and run vaccination clinics at the workplace.

• Pay for it.
Vaccination Certifications

• While the enforcement of such mandates wouldn’t be without its challenges, it would hardly be impossible or without precedent. To board an emirates flight to Dubai today, for example, all passengers must present a negative COVID-19 test certificate.

• Once a vaccine is available, airlines could put in place sweeping regulations requiring COVID-19 vaccination certificates.

• Similarly, governments may require proof of a COVID-19 vaccination to get a passport which would reflect such vaccination status. Driver’s licenses could be updated in a similar fashion.

• At work, employee badges could carry vaccination stickers, and a paper certificate from your doctor could serve as vaccine proof for public events.
Lessons From The Past

Lessons from HIV contact tracing

• Both viruses can be spread by people who are asymptomatic and do not know their status
• Both viruses are having a more devastating impact on already marginalized communities, including communities of color.
• With both epidemics, we have seen scapegoating and blame, and egregious disparities in enforcement of public health restrictions by police.

Lessons from September 11, 2001

• Lost civil liberties are hard to regain.
• Some companies are betting on the technology outlasting the crisis; as one manufacturer wrote, “we believe the demand for viable solutions like these will last far longer than most people think. Just like 9-11 and how it impacted and changed air-travel forever, this too will change the way we live and work for a long time to come.”
The COVID-19 Consumer Data Protection Act would:

- Require companies under the jurisdiction of the federal trade commission to obtain affirmative express consent from individuals to collect, process, or transfer their personal health, geolocation, or proximity information for the purposes of tracking the spread of COVID-19.
- Direct companies to disclose to consumers at the point of collection how their data will be handled, to whom it will be transferred, and how long it will be retained.
- Establish clear definitions about what constitutes aggregate and de-identified data to ensure companies adopt certain technical and legal safeguards to protect consumer data from being re-identified.
- Require companies to allow individuals to opt out of the collection, processing, or transfer of their personal health, geolocation, or proximity information.
- Direct companies to provide transparency reports to the public describing their data collection activities related to COVID-19.
- Establish data minimization and data security requirements for any personally identifiable information collected by a covered entity.
- Require companies to delete or de-identify all personally identifiable information when it is no longer being used for the COVID-19 public health emergency.
- Authorize state attorneys general to enforce the Act.
Public Health Emergency Privacy Act

• The Act would protect “emergency health data” which means “data linked or reasonably linkable to an individual or device, including data inferred or derived about the individual or device from other collected data provided such data is still linked or reasonably linkable to the individual or device, that concerns the public COVID–19 health emergency.”

• Examples of such data include:
  • information that reveals the past, present, or future physical or behavioral health or condition of, or provision of healthcare to, an individual, including data derived from testing an individual such as COVID-19 viral or serological test results, along with genetic data, biological samples, and biometrics;
  • other data collected in conjunction with other emergency health data or for tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the COVID–19 public health emergency, such as (i) geolocation data, (ii) proximity data; and (iii) any other data collected from a personal device.

• If enacted, the Federal Trade Commission (FTC) would promulgate rules regarding data collection, use and disclosure under the Act. In addition, both the FTC and state attorneys general would have enforcement authority over the Act.

• Because there is no comprehensive Federal privacy law, this Act, if passed, would be a temporary crisis measure that would be terminate once COVID-19 was no longer deemed a public emergency. Covered organizations would be required to not use or maintain emergency health data 60 days after the termination of the public health emergency, and destroy or render not linkable such data.
Key Requirements of the Act for "Covered Organizations":

- Only collect, use or disclose data that is necessary, proportionate and limited for a good-faith health purpose;
- Take reasonable measures, where possible, to ensure the accuracy of data and provide a mechanism for individuals to correct inaccuracies;
- Adopt reasonable safeguards to prevent unlawful discrimination on the basis of emergency health data;
- Only disclose data to a government entity if it is to a public health authority and is solely for good faith public health purposes;
- Establish and implement reasonable data security policies, practices and procedures;
- Obtain affirmative express consent before collecting, using or disclosing emergency health data, and provide individuals with an effective mechanism to revoke that consent. **NOTE**: There are limited exceptions where consent is not required including to protect from fraud/malicious activity, to prevent a security incident, or if otherwise required by law;
- Provide notice in the form of a privacy policy prior to collection that describes how and for what purposes the data will be used (including categories of recipients), the organization’s data security policies and practices, and how individuals may exercise their rights.
Exposure Notification Privacy Act

ROLE OF PUBLIC HEALTH AUTHORITIES

• The act will require that public health officials be involved with the deployment of any exposure notification systems. The act will prohibit any automated exposure notification service not operated by or in collaboration with a public health authority. This would give users confidence that the technologies they are using are legitimate and not created by unqualified actors.

• The act will allow only medically-authorized diagnoses of infectious diseases to be submitted to exposure notification systems. This will guard against false reports.

INDIVIDUALS RIGHTS

• The act will require that participation be voluntary and based on affirmative, express consent. Further, consent could be withdrawn at any time.

• The act will allow participants to delete their data from an exposure notification system at any time.

• The act will make it unlawful to discriminate against, or otherwise make unavailable to an individual, any place of public accommodation based on data collected or processed through an automated exposure notification service. This will bar people from being prevented from entering a public place if they chose not to sign up for a coronavirus exposure notification app.
DATA RESTRICTIONS TO PRESERVE PRIVACY

• The act will limit the collection and use of data to that which is necessary for the purpose of the system and prohibit any commercial use of data.

• The act will prohibit operators of automated exposure notification services from collecting or using data beyond what is necessary to implement such services for public health purposes. Operators would be prohibited from collecting or processing data for any commercial purpose.

• The act will create strong cybersecurity and breach notification safeguards. In order to protect user data, the legislation creates comprehensive data security requirements and obligations to immediately notify individuals in the event of a security incident.

• The act will require recurring and ongoing data deletion obligations.

• The act will make allowances for public health research.

ENFORCEMENT

• The act will empower the FTC and state attorneys general to pursue violators.

• The act will allow the FTC to pursue civil penalties for first-time violations.

• The act will protect state privacy rights, ensuring that consumer privacy and health laws remain in place.
Questions?
Technology and Liberties in the Fight Against Coronavirus

We need to continue to think creatively about how new technology can help us fight this disease, but we also need to remain skeptical before we compromise our civil liberties.

Jay Stanley, Senior Policy Analyst
May 19, 2020

There have been disease outbreaks throughout human history, but never one that has taken place in the era of high-tech tracking tools and “big data.”

Policymakers and technologists have proposed a number of ideas for leveraging such technologies to help suppress the spread of COVID-19. At the ACLU, we recognize the urgency of stemming the pandemic and re-opening America, and don’t think we should immediately write off any tools that may offer public health benefits. But we shouldn’t give up critical rights and freedoms unless a proposal is necessary, effective, and proportionate. We are particularly wary of technological solutions that would
interfere with or divert resources away from public health solutions with proven effectiveness, or that risk exacerbating existing disparities that have already led to inequitable health outcomes.

A review of the most prominent proposals that have been put forward suggests that we need to remain vigilant lest we give away our liberty and get little in return. Here are just a few examples:

**Tech-Assisted Contact Tracing**

Perhaps the most prominent discussion about using technology to help fight the coronavirus has revolved around how high-tech tools can augment contact tracing. One of the oldest and most basic techniques for slowing the spread of disease, contact tracing involves tracking an infected person’s past interactions so that those who may have been exposed can be identified.

Early proposals to use cell phone location tracking data have rightly been dismissed. Mobile phone location data is not nearly accurate enough for identifying those who had been exposed to an infected person. And even if it were, this data (much of which is gathered by shady companies that sneak tracking software into phone apps) is collected through a variety of technologies and is scattered among a variety of companies. Attempts to deploy this concept have not gone well.

A more viable proposal has centered around using our smartphones’ Bluetooth technology to allow phones to detect other phones that come nearby, and use that to automatically keep track of who may have been exposed to an infected person. If done right, this approach can be more privacy-protective because it does not require the collection of sensitive location data and stores data locally and in ways that don’t identify people. The Bluetooth-enabled approach gained traction when Apple and Google announced they were teaming up to create such a system.

While we have a lot of skepticism about whether this concept is likely to prove practical, we have outlined a set of technology principles that the public and developers should use to assess any such proposal. We have also outlined principles that should inform policies and procedures governing the use of these untested technologies.
which are not permitted by the FAA to be flown over people or beyond the line of sight of the operator — is more likely to acclimate people to drone surveillance than it is to slow COVID. The use of drones in this manner over homeless encampments in California has also drawn criticism from homeless advocates, who say it is a terrible way to approach the unhoused.

**Immunity Passports**

Another proposal for how to use technology against COVID is to create an infrastructure for so-called “immunity passports.” The idea, appealing at first blush, is to speed reopening by allowing people who are immune to COVID to have a way to certify that fact so that they don’t have to be subject to all the restrictions now in place. The problem, as we have outlined, is that the science is not there to support that approach, and that it would divide workers into two classes. One group, those with COVID immunity, would be given preferential access to employment, housing, or public accommodations.

This new class system would incentivize people, particularly the economically vulnerable, to risk their health by getting COVID-19 so they could get a passport and return to work. It would also likely worsen existing racial, disability, and economic disparities in America. Any immunity passport system would also likely endanger our privacy rights by creating a new surveillance infrastructure to collect health data.

**Remote Learning**

Finally, technology has come to play a central role in education during the COVID crisis — and that has intensified some of the privacy and discrimination problems that technology often brings. A lot of school districts are distributing software that spies on the students it’s supposed to help. We have called on school districts to require these educational technology companies to disable any surveillance functions and limit their personal information gathering to only what is directly necessary for their products to work. We’re also calling on Congress and state and local governments nationwide to give all students equal access to the technologies that make effective remote learning possible. That includes funding to meet the broadband access and technology needs of students and people with low income.

***

The great 20th-century scientist Linus Pauling once said, “If you want to have good ideas you must have many ideas. Most of them will be wrong, and what you have to learn is which ones to throw away.” We need to continue to think creatively about how new technology can help us fight this disease and get back to normal, but we also need to remain skeptical before we compromise our civil liberties, realizing that there will be a lot of ideas that do need to be thrown away. Others may have promise but need to be implemented only with great care.

In the age when everyone looks to data and technology as the solution to all problems, the biggest
Fever Detectors

Another technology that is receiving a lot of attention is fever detection, which we have also analyzed in a white paper. Temperature screening is seen by public health experts as having very limited usefulness — many infectious people do not have a fever, and the technology is not very accurate — but companies and others are rushing to deploy it.

Temperature checks should not be deployed unless public health experts say conclusively that they will help. We don't want to see a world where inaccurate tests disrupt people’s lives and invade their privacy, or waste time and other resources that could be better used in fighting the pandemic. If public health experts conclude temperature screenings will help, measures must be taken to minimize disruption and ensure fairness, and the use of remote temperature screenings must end with the outbreak. At no point should we deploy remote mass temperature screening using thermal cameras. That technology has both the least accuracy and the most potential to be diverted to other, privacy-invasive uses once COVID-19 is gone.

Drones

One proposed deployment of thermal scanners is in drones — another tool that is being pushed to combat the pandemic. Our research makes clear that putting thermal scanners on drones makes them laughably inaccurate for fever detection. Drones are also being deployed in other ways that seem more silly than anything. Drones have been sighted flying over parks to look for social distancing violations (how can it know which people are members of the same household?) and shout admonishments at those who appear to be in violation, for example. The use by police of these loud, short-battery life devices —
solutions to the current crisis, according to public health experts, remain relatively low-tech: soap and water, widespread testing, access to health care, social distancing, old-fashioned human contact tracing, and, ultimately, a treatment or vaccine.
June 16, 2020

Mr. Sundar Pichai  Mr. Tim Cook
Chief Executive Officer  Chief Executive Officer
Google, LLC  Apple, Inc.
1600 Amphitheatre Parkway  1 Apple Park Way
Mountain View, CA 94043  Cupertino, CA 95014

Dear Mr. Pichai and Mr. Cook:

The undersigned Attorneys General ("State Attorneys General") write to express our strong concerns regarding the proliferation of contact tracing apps on your platforms that do not sufficiently protect consumers’ personal information. Digital contact tracing may provide a valuable tool to understand the spread of COVID-19 and assist the public health response to the pandemic. However, such technology also poses a risk to consumers’ personally identifiable information, including sensitive health information, that could continue long after the present public health emergency ends.

We are aware of your companies’ joint development of application programming interfaces (APIs) that may be used to build decentralized exposure notification and contact tracing apps that utilize Bluetooth. Additionally, we understand from press reports and online materials that those APIs will only be available to public health authorities and that use of the APIs will be contingent on the inclusion of certain features to protect consumer privacy.

While we welcome your stated focus on a privacy-centered notification and tracing tool for future use, several COVID-19 related contact tracing apps are already available on Google Play and the App Store. Some of those apps may endanger consumers’ personal information. We are particularly concerned about purportedly “free” apps that utilize GPS tracking, contain advertisements and/or in-app purchases, and are not affiliated with any public health authority or legitimate research institution.¹

Moreover, as public health authorities release apps built with your APIs, there is likely to be increased media and consumer attention on exposure notification and contact tracing apps. Other developers may take advantage of the situation by placing new contact tracing apps on your platforms that do not adequately safeguard consumers’ personal information.

¹ For instance, as recently as early May, the first result when a consumer searches “contract tracing” on both platforms was an app called “Contact Tracing” developed by Piusworks, LLC, a California company with a suspended registration. According to the app information previously disclosed on Google Play, Contact Tracing uses geolocation tracking, contains ads, and offers in-app purchase, and it has been installed over 50,000 times. The app has since been removed from Google Play but is still available on the App Store.
in compliance with our states’ laws. Therefore, we urge Google and Apple to take the following actions with respect to exposure notification and contact tracing apps available to U.S. consumers on Google Play and the App Store:

1. Verify that every app labeled or marketed as related to contact tracing, COVID-19 contact tracing, or coronavirus contact tracing or exposure notification is affiliated with a municipal, county, state or federal public health authority, or a hospital or university in the U.S. that is working with such public health authorities;

2. Remove any app that cannot be verified consistent with the above; and

3. Pledge to remove all COVID-19 / coronavirus related exposure notification and contact tracing apps, including those that utilize your new APIs, from Google Play and the App Store once the COVID-19 national emergency ends. In addition, provide written confirmation to our offices that the apps have been removed or an explanation why removal of a particular app or apps would impair the public health authorities affiliated with each app.

Implementing these limited measures could help protect the personally identifiable information and sensitive health data of millions of consumers during this crisis.

Sincerely,

Douglas Peterson
Nebraska Attorney General

Ellen F. Rosenblum
Oregon Attorney General

Kevin G. Clarkson
Alaska Attorney General

Leslie Rutledge
Arkansas Attorney General

Xavier Becerra
California Attorney General

Phil Weiser
Colorado Attorney General

William Tong
Connecticut Attorney General

Kathleen Jennings
Delaware Attorney General

---

2 This refers to the expiration of the emergency declared by the Secretary of Health and Human Services on January 31, 2020, under section 319 of the Public Health Service Act (42 U.S.C. 247d), and any renewals thereof.
Karl A. Racine  
District of Columbia Attorney General

Leevin Taitano Camacho  
Guam Attorney General

Clare E. Connors  
Hawaii Attorney General

Lawrence Wasden  
Idaho Attorney General

Kwame Raoul  
Illinois Attorney General

F. Aaron Negangard  
Indiana Chief Deputy Attorney General

Tom Miller  
Iowa Attorney General

Derek Schmidt  
Kansas Attorney General

Jeff Landry  
Louisiana Attorney General

Aaron M. Frey  
Maine Attorney General

Brian Frosh  
Maryland Attorney General

Maura Healey  
Massachusetts Attorney General

Dana Nessel  
Michigan Attorney General

Keith Ellison  
Minnesota Attorney General

Aaron D. Ford  
Nevada Attorney General

Gordon MacDonald  
New Hampshire Attorney General

Gurbir S. Grewal  
New Jersey Attorney General

Hector Balderas  
New Mexico Attorney General
The Limits of Location Tracking in an Epidemic

By Jay Stanley and Jennifer Stisa Granick
April 8, 2020

As Americans struggle to confront the COVID-19 outbreak, some have suggested that cell phone location tracking technology can help in the effort to contain the disease. The tech industry and the White House are reportedly having conversations over how information technology might be deployed, and there is increasing discussion about how foreign countries are using technology. The governor of Florida has even floated the idea of using an app to track visitors from COVID-19 hotspot New York.

However, policymakers must have a realistic understanding of what data produced by individuals’ mobile phones can and cannot do. As always, there is a danger that simplistic understandings of how technology works will lead to investments that do little good, or are actually counterproductive, and that invade privacy without producing commensurate benefits.

As we write this white paper, public health experts say that the nation has three urgent needs: strong social distancing measures, widespread testing capability, and material support for hospitals being overwhelmed by victims. However, once our hospitals reach a point where they’re able to handle the stream of new patients, experts say that indiscriminate population-wide social distancing measures may give way to a new phase: chronic, lower-level waves of infection in which a combination of widespread testing, individualized quarantine orders, and traditional epidemiological contact tracing once again become a principal means of combatting the disease. It would be in such a period — the window between the end of the initial wave and the development of a vaccine — that using certain forms of data generated by cell phones — such as location histories or records of proximity to other devices — might make sense.

The challenges posed by COVID-19 are extraordinary, and we should consider with an open mind any and all measures that might help contain the virus consistent with our fundamental principles. We note some of those possible uses in this paper. At the same time, location data contains an enormously invasive and personal set of information about each of us, with the potential to reveal such things as people’s social, sexual, religious, and political associations. The potential for invasions of privacy, abuse, and stigmatization is enormous. Any uses of such data should be temporary, restricted to public health agencies and purposes, and should make
the greatest possible use of available techniques that allow for privacy and anonymity to be protected, even as the data is used.

Because location tracking has such ominous potential implications, in short, we should make sure that any uses of such sensitive data are necessary, effective, and proportionate. The principal focus of this paper is on whether such uses would be effective.

**Key Questions**
The likely effectiveness of different uses of cell phone location data hinges on exactly how each is envisioned as being used in the effort to stem the spread of the coronavirus. Important variables are:

1. **What is the goal?** Is it tracking overall trends, helping people who have tested positive recall past contacts, identifying unknown individuals who may have been infected by the patient, or enforcement of quarantines or stay-at-home orders?
2. **What data?** Is it aggregate and anonymized data, or individually identifying information? How precisely can the information pinpoint individuals’ locations? Is the dataset complete enough that one can draw meaningful conclusions? Will the data under- or mis-represent people of color or low-income communities in a manner that could lead to prejudicial results, such as inferior access to health care or over-policing?
3. **Who gets the data?** Does the government get access to the raw data, is it shared only with public health entities such as qualified academics or hospitals, or does it remain in the hands of the private entity that originally collected it?
4. **How is the data used?** Is it used for centralized government action, such as issuing or enforcing quarantine orders, or for punitive measures? Or, does it enable decentralized individual decision-making such as checking announcements of possible exposure points and choosing to go to a testing center?
5. **What is the life cycle of the data?** Any corpus of data is likely to create risks to the people it represents. A responsible steward of other peoples’ data will have plans for data destruction once the data’s relevance is diminished, to mitigate future compromise.

The answers to these key questions vary widely for the different proposals that have been the center of recent discussions. Now, we turn to each of these proposals and consider them in light of the key questions.

**Proposed Use: The use of mass location data to identify unknown individuals who may have been exposed to a contagious person**
One often-mentioned idea is to gather mass location data on as many people as possible and analyze that data with the goal of identifying those who have been exposed to an infected person. Under this vision, the location record of a newly discovered coronavirus-positive person would be matched against everyone else’s location records, and those who were near the infected person would be notified, tested, and/or ordered into quarantine. This kind of tracking is part of what China has been doing in its seemingly successful effort to suppress the virus,
which has fed the appeal of such tracking. Israel has also revealed that its government has been secretly retaining detailed cell phone location records on its population, and has begun trying to use them in this way against COVID-19. And “about a dozen” other countries are reportedly testing the same concept through a product created by a notorious spyware company.

There are serious practical problems with this concept, however.

**Data on individuals’ locations is not accurate enough for automated contact tracing.**

We have spoken with engineers and executives at a number of the largest U.S. companies that hold location data on Americans’ movements and locations, and generally they have told us that their data is not suitable for determining who was in contact with whom for purposes of COVID-19 contact tracing.

Data on Americans’ movements and locations is collected through various technologies:

- **Cell tower location data.** Cellular phones continuously emit signals to identify themselves to nearby towers or other cell sites so that the system can route data and calls their way. Each time a phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). Wireless carriers collect and store this information. Because the carrier knows the physical location of the cell tower, this data has the side effect of telling telecom providers approximately where those phones are. The precision of cell-site location information varies depending on the strength of the signal, the density of towers, network load and other factors. Numerous data entries over time can support an inference that a phone was near a particular location at a certain point in time. They can also show when a phone is moving in a particular direction — for example, southbound on highway 101. But the data is not precise enough to tell you how close two phones are to each other. In rural areas the information may place people only in a several-square-mile area. In urban areas, where towers are more densely deployed, the accuracy is typically higher, but still insufficient for reliably pinpointing location. China reportedly looked into using cell-site location data in its fight against COVID-19 but found that it was too inaccurate, generated too many false positives, and was wasting manpower.

- **GPS.** When mobile phones have satellite sensing turned on, they can identify their own location with a best-case theoretical accuracy of 1 meter, but more typically 5 to 20 meters under an open sky. GPS radio signals are relatively weak; the technology does not work indoors and works poorly near large buildings, in large cities, and during thunderstorms, snowstorms, and other bad weather. It can also take a GPS receiver up to several minutes to perceive its location when first turned on or brought outdoors. In addition, phones receive transmissions from GPS satellites, but they do not automatically calculate, save, or broadcast GPS location information. That only happens when a user installs an app on their phone that is designed to do that. Those apps may send that data to dozens of different companies or to none at all; there is not a single repository.
• **Wi-Fi, Bluetooth, and other radio location.** Google and other companies hold databases identifying Wi-Fi router locations, and use that information in combination with GPS data to help locate phones with more precision than can be done with GPS alone. Bluetooth, the wireless technology used to exchange data over short distances (less than 30 feet), is also **widely used for tracking**, especially in stores. But not all phones have Bluetooth turned on by default and Bluetooth contacts do not comprise anything like a comprehensive tracking system.

• **QR codes.** In China, residents are required to install an app on their phone that they **must use** to scan **QR** codes that have been placed in taxis and at the entrances of buildings, buses, and subway stations. These real-world checkpoints provide far more reliable and accurate tracking than wireless technologies — and can be combined with those technologies. The United States, however, has no such checkpoint infrastructure in place, little capacity or apparent desire to build one, and no legal authority to compel people to carry a phone, much less install a specific app on their phone.

The CDC warns against coming in “close contact” with a person who has tested positive for the virus, defining close contact as “being within approximately 6 feet (2 meters), of a person with COVID-19 for a prolonged period of time.” None of the data sources discussed above are accurate enough to identify close contact with sufficient reliability. None are reliably accurate to within 6 feet. Using the wrong technology to draw conclusions about who may have become infected might lead to expensive mistakes such as two week isolation from work, friends, and family for someone — perhaps even a health care worker or first responder — who was actually not exposed. Israel’s use of location data has already sparked complaints about accuracy.

A location tracking system over time can be accurate enough to place a person near a bank, bar, mosque, clinic, or other privacy-sensitive location. But the fact is, commercial location databases are compiled for advertising and other purposes and are simply not accurate enough to reliably determine who was in close contact with whom.

**The algorithms are not likely to be reliable.**

Even if we were to imagine a set of location data that had pinpoint accuracy, there would still be problems translating that in any automated way into reliable guesses about whether two people were in danger of transmitting an infection. The Israeli system apparently acts on the basis of nothing more than an automated look at proximity. In Israel, one woman was identified as a “contact” simply because she waved at her infected boyfriend from outside his apartment building — and was **issued a quarantine** order based on that alone. Such a system is likely to make many such mistakes; it won’t know that a bank teller is shielded from transmission because they’re behind plexiglass, or that two people close together in a building are actually in separate apartments divided by a wall.

The alternative is to try to make more educated guesses by taking account of such circumstances as well as such factors as the duration of a contact and the number of days the positive-testing person has been infected. But those guesses will inevitably be highly unreliable.
Ambitious plans for automated recording and analysis of human life are everywhere these days, but few such efforts are reliable because human life is messy, complicated, and full of anomalies.

*The data is fragmented and may be biased.*

Complicating matters further, no single, centralized party holds the location data generated by Americans. Most location data with any level of precision is generated by an essentially *corrupt ecosystem* of shady, privacy-invading companies that engage in mass location tracking without individuals’ meaningful awareness or consent, typically by paying the developers of smartphone apps to hide tracking capabilities inside those apps. This location data is scattered among *dozens* of such companies most Americans have never heard of. And giants like Google and Facebook that collect location data have enormous reach within the population, but only have location data on a minority of their users. Any kind of automated contact tracing that hopes to find close contacts will need to access more than a slice of existing data pools if the tracking is to effectively find otherwise unknown infected people.

There may also be differences in how various populations and demographics are represented in the data. Making public health decisions on such datasets could leave out entire populations, and misrepresent others, and lead to a deployment of health care resources that is not only biased and unjust — tilted toward wealthy neighborhoods, for example — but ineffective from a public health standpoint.

**Proposed Used: The use of specific location data to assist in identifying where an infected person was in the recent past**

Location data is more effective when used to trigger a patient’s recollection of places traveled in the past. *South Korea* has so far *succeeded* in minimizing its outbreak through a massive testing and contact-tracing program without the kinds of lockdowns and business closures that other countries have resorted to. One element of its contact-tracing effort is retracing the steps of newly identified coronavirus carriers. To help do that, the legislature has passed a law giving the government authority to collect location data from those who test positive. But instead of trying to cross-reference the location histories of infected people against massive population-wide location datasets, South Korean officials simply “anonymize” and *publish* the patients’ location histories. Numerous web sites and apps make that information available, and citizens can check for possible collisions with infected people. Widespread and quick testing is available for anyone worried that they have been exposed. Such checks have become a part of daily life in South Korea.

Similar mechanisms have been part of the solution in China. Baidu (a Chinese analogue to Google) created a map layer on top of its standard mapping app that shows real-time locations of confirmed and suspected cases of the virus so that people can avoid more-affected areas. Another company, Qihoo 360, launched a platform where travelers can check if anyone on their recent train or plane trips has since tested positive.
One problem that has emerged in South Korea is that the authorities are not doing a good job anonymizing the data. One alert informed the public, for example, of a “43-year-old man, resident of Nowon district” who was “at his work in Mapo district attending a sexual harassment class.” Unsurprisingly some people described in such ways are being identified by members of the public. That has reportedly left many people more afraid of social humiliation than of the disease itself, threatening to interfere with testing, arguably the most important intervention to control the virus.

In fact, data scientists have learned in recent years that it is surprisingly difficult to anonymize data. That is doubly true with regard to location data, because people reveal themselves by where they go; even relatively rough information about a person’s location will often identify them uniquely. For example, according to one study, just knowing the zip code (actually census tract, which is basically equivalent) of where you work and where you live will uniquely identify 5 percent of the population. If you know the “census blocks” where somebody works and lives (an area roughly the size of a block in a city, but larger in rural areas), the accuracy is much higher, with at least half the population being uniquely identified. And of course, once a person’s home address is identified, little doubt as to their identity remains.

Even without robust unique identification, stigma and harassment could follow. Imagine four different people who all live in ZIP code A and work in ZIP code B: Even if they are not uniquely identified, if one tests positive and their location data is published, the other three may fall under suspicion as well.

That said, information about the times and places where infected people were present could certainly be aggregated and anonymized far more effectively than South Korea has done. And there are ways to use location data that don’t involve publishing it — for example, it could simply be used in cooperation with those who are infected to jog their memories and help them retrace their movements.

**Proposed Use: The use of aggregate location data**

The use of anonymous aggregated location data could help epidemiologists answer questions such as how many people are moving between adjacent neighborhoods, towns, or states each day, or how much the average resident of an area changes their travel after new movement limitations are imposed. The CDC and state and local governments in the U.S. are reportedly receiving some such data from the mobile advertising industry.

Aggregate location data does not usually reveal individuals’ private information (though there can be exceptions, such as in sparsely populated areas where the numbers are so small that they can reveal an identifiable person’s movements). Of course, some party needs to hold the raw data before it is aggregated. Though such data could theoretically be generated using privacy-protecting software built into the collection mechanisms, few players in this ecosystem have the incentive to utilize such mechanisms. So far, the sources of underlying location data in
the aggregate applications we’ve seen are unsavory — this is data surreptitiously collected via mobile ads and funneled through a location data broker.

One question is who sees what. Ideally, nobody sees anything more than they need. For example, a public health official who needs to know how many people travel daily to her town from a nearby COVID-19 hotspot does not need access to her fellow residents’ personalized travel data to find that out. In many cases, the entity that already holds the location data can keep it and the government need not receive a copy. Any entity should be transparent and open about where the data came from, who holds it, and how it is being analyzed.

Another question is what officials do with the insights that even anonymous and aggregated data can generate. Encouraging voluntary social distancing is one thing; increasing police interventions in non-compliant zip codes is another. Will the data create misleading pictures of behavior within communities of color or low-income communities in a manner that could lead to prejudicial results, such as inferior access to health care or over-policing?

Proposed Use: Enforcement

Another possible use of location information is in the enforcement of quarantines, shelter-in-place orders, and travel restrictions. These uses contemplate turning people’s cell phones into ersatz ankle monitors.

As a technological matter, the accuracy of cell phone location data is adequate for detecting people who move any significant distance from their homes, or who are traveling from another place.

Aggregate data could also be used to enforce compliance with stay-at-home orders. For example, companies could notify the authorities when cell phone data suggested that people were gathering in numbers prohibited by local public health measures, without sharing the identities of those who appear to have gathered, such as at a rogue bar that appeared in Los Angeles during a shelter-in-place regime. Such measures would have to be used with care lest multi-story apartment buildings or the like trigger alarms.

Public health experts caution, however, that a law enforcement approach to combatting disease is less effective than relying on voluntary measures and compliance. That is because an enforcement approach often sparks counterproductive resistance and evasion and tends to sour the relationship between citizens and their government at a time when trust is of paramount importance. Good public health measures leverage people’s own incentives to report disease and help stop its spread.

Indeed, where people feel that their phones have become an instrument of an antagonistic government, there are a number of technological steps they might take to defeat that tool. The simplest step would be to turn the location function off on their phone, or turn their phone off
entirely. Uncooperative subjects could also simply leave their phones at home, or acquire and register a second, dummy phone that is not their primary device which they leave at home.

It is probably to forestall such stratagems that Hong Kong is issuing electronic tracker wristbands to people under compulsory home quarantine to ensure they do not go out. In Taiwan, an American University student under quarantine received a visit from police after his battery died while he slept. To be effective, that kind of close monitoring of cell signals at scale would require either significant manpower and resources or the creation and implementation of automated detection capabilities, and the administrative structures required to back them up — all well before the arrival of a vaccine rendered them superfluous.

**Other Possible Concepts and Models**

There may be many other ways of using cell phone data that have not yet been fully explored. For example, in Singapore, an app called TraceTogether uses short-range Bluetooth signals to keep track of which other people come nearby over time. If a user later turns out to be positive, their phone then holds an encrypted record of who else was nearby, which can be unlocked by Singapore’s Ministry of Health. Rather than relying on location tracking, they are instead using “proximity tracking.”

There are a number of problems with the concept. In Singapore, the Ministry of Health has access to user data about every app user, and detailed access to activity and contact logs and from every infected user. While they’ve promised to use this access only for public health purposes, there is nothing stopping them from turning over data to law enforcement or other punitive agencies. Also, for the app to be effective in its public health goals, it would need a certain level of adoption by the public, which might be averse to installing it out of fear of these punitive measures. Other open questions include whether Bluetooth is precise enough to distinguish close contacts given that its range, while typically around 10 meters, can in theory reach up to 400 meters, and that its signal strength varies widely by chipset, battery, and antenna design.

It may be possible, however, to design implementations that address some or all of these problems and adhere to important principles such as voluntariness, decentralization, simplicity, transparency, and the lack of reliance on a persistent identifier. Such implementations would enjoy increased adoption and effectiveness because they would engender public trust. A number of developers are working on such implementations with the welcome goal of being both privacy-preserving and effective.

And of course, there may be other ideas for leveraging technology that no one has yet conceived.
Conclusion
In this crisis, we need to seriously consider how technology might help improve public health. This investigation must be based on a realistic understanding of what technology and data can and cannot do, lest we divert attention, expertise, and financial resources from other, simpler but time-tested methods that are more effective. In particular, policymakers should understand the limits of existing location data and devices for automated contact tracing.
Tracking Apps are Unlikely to Help Stop COVID-19

The debate over using apps for contact tracing or exposure warnings to help fight COVID-19 is largely a sideshow to the principal coronavirus health needs.

Proposals to use the tracking capabilities of our cell phones to help fight COVID-19 have probably received more attention than any other technology issue during the pandemic. Here at the ACLU, we have been skeptical of schemes to use apps for contact tracing or exposure warnings from the beginning, but it is clearer than ever that such tools are unlikely to work, and that the debate over such tracking is largely a sideshow to the principal coronavirus health needs.

We have said from the outset that location-based contact tracing was untenable, but that the concept of “proximity tracking” — in which Bluetooth signals emitted by phones are used to notify people who may have been exposed — seemed both more plausible and less of a threat to privacy. Indeed, a number of
serious institutions began working on this concept early in the pandemic, most notably Apple and Google, which have already implemented a version of the concept in their mobile operating systems.

Some of the problems with tech-assisted contact tracing have been apparent from the beginning, such as the social dimensions of the challenge. Smartphone ownership is not evenly distributed by income, race, or age, threatening to create disparate effects from such schemes. And even the most comprehensive, all-seeing contact tracing system is of little use without social and medical systems in place to help those who may have the virus — including access to medical care, testing, and support for those who are quarantined. Those systems are all inadequate in the United States today.

Other problems with technology-assisted contact tracing have become more apparent as the pandemic has played out. Specifically, such tracing appears to be squeezed from two directions. On the one hand, a tool shouldn’t pick up every fleeting encounter and swamp users with too many meaningless notifications. On the other, if it is confined to reporting sustained close contacts of the kind that are most likely to result in transmission, the tool is not likely to improve upon old-fashioned human contact tracing. Those are the kinds of contacts that people are likely to remember. And those memories, relayed to human contact tracers, are more likely to identify a patient’s significant past exposures than an automated app that can’t determine, for example, whether two people were separated by glass or a wall.

A difficult disease to trace

The first problem — the danger of generating far too many “exposure notifications” — is considerable. As one commentator put it, “actual transmission events are rare compared to the number of interactions people have.” Swamping users with false notifications would be useless and annoying at best, and seriously disruptive and counterproductive at worst. Ultimately, people will stop taking the notifications seriously, or just uninstall the app.

That problem is made worse by the fact that COVID-19 is a more difficult disease to trace than many. As a group of prominent epidemiologists from the University of Minnesota explained in a report on contact tracing, contact tracing is less effective when:

1. Contacts are difficult to trace, such as when a disease is transmitted through the air. Respiratory transmission appears to be the primary way COVID-19 is transmitted. Compared to the kind of contact tracing that has long been done with HIV, where transmission takes place through sex or blood, the virus that causes COVID-19 is much harder to track. One cough or sneeze from a stranger may be enough to infect an unlucky passerby — as can sharing an interior space with a “super-spreader” who is on the other side of a large room.

2. The infection rate in a community is high. In the United States, as of this writing (July 2020), there are currently around 50,000 new coronavirus cases being identified every day. As the Minnesota
report puts it, “contact tracing is most effective either early in the course of an outbreak or much later in the outbreak when other measures have reduced disease incidence to low levels.” The U.S. may someday reach the point where cases are once again sporadic rather than widespread, but for now experts recommend concentrating contact tracing on contacts within households, healthcare and other high-risk settings, and case clusters — an approach much more amenable to manual contact tracing.

3. A large proportion of transmissible infections are from people without symptoms. In May the CDC estimated that 40 percent of new COVID-19 infections come from asymptomatic carriers.

The Technology is Not Reliable Enough

These factors increase the risk of generating too many exposure notifications to be useful. Serious technical challenges with using smartphones for contact tracing also increase that risk. One of the biggest questions has always been how to use Bluetooth to judge which encounters are worthy of being recorded as potential transmission events. Judgments have to be made about how close a person needs to be, and for how much time, to meet the warning threshold. That becomes even trickier since Bluetooth can’t reliably measure distances. The strength of a Bluetooth signal varies not only with distance, but also from phone to phone, and from owner to owner. The frequency at which Bluetooth operates (2.4 GHz) is one that is easily absorbed by water, including the water in the human body, which means that signal strength can vary significantly depending upon whether a person has their phone in their front or back pocket, and how much that person weighs.

Complicating matters is the fact that existing contact-tracing apps are being thrown together very quickly. Google and Apple moved from concept to a finalized product in less than 12 weeks. They should be commended for stepping up in an emergency, but we shouldn’t expect it to work well anytime soon. As is clear to any experienced software developer, their product is basically an early prototype that’s being pushed into production. In a normal world, they would be testing their app on groups of hundreds and then thousands of people in cities and a variety of other real-world situations. Through no fault of Apple and Google, there simply hasn’t been the opportunity to do the kind of engineering development and refinement that a project like this really needs.

And of course, what is true of software developed by Apple and Google is even more true of apps developed in a rush by state governments like North Dakota and Rhode Island, or other nations like South Korea. South Korea has been lauded for its high-tech coronavirus response. But the quarantine app the country has been using put people’s names, locations, and other private information at risk by failing to follow basic cybersecurity practices.

Compliance

While effective technology-assisted contact tracing apps must avoid generating too many exposure notifications, they must also establish that they can improve upon or significantly augment old-
fashioned human contact tracing.

Epidemiologists emphasize that contact tracing has always been a tricky and sensitive job. Getting people to trust any official enough to open up about their potentially privacy-sensitive whereabouts and contacts is a skill — one that requires “training and development of a specialized skill set” as well as “consideration of local contexts, communities, and cultures.”

That is especially true since those who are identified as having been exposed to the coronavirus are asked to self-quarantine for two weeks — putting much or all of their life on hold, and possibly risking the loss of a job or income, necessitating the finding of new caregivers for dependents, and imposing various other costs. That’s something that a friend will be reluctant to impose upon another friend by giving their name — especially where no social support is provided to those asked to self-quarantine. As the Minnesota report warned, “If people perceive the economic, social, or other costs of compliance with contact tracing are greater than its value, it won’t be successful.”

There are many reasons to doubt that these tricky issues can be navigated better through technology. As report co-author Michael Osterholm put it, “Having been in public health for 45 years, and having cut my teeth in surveillance in many different ways — I don’t think most people would comply. If I got notifications that I’d been exposed to [someone] with COVID, would I self-isolate for 14 days at home, because I got a text on my phone?”

The sensitive privacy and trust issues that human contact tracers face are likely to be amplified in the technology realm. People who are reluctant to tell contact tracers where they’ve been are likely to be even more reluctant to let an app carry such information. By building tools with very strong, cleverly constructed privacy protections, Apple, Google, and others have created the best possible chance of engendering trust in those apps, but those protections still have gaps. People who refuse to wear a mask are unlikely to deliberately install tracking software on their phone, whatever privacy assurances they are given. Nor are many members of Black, Brown, and immigrant communities for whom “trust in the authorities is non-existent.”

Some experts have estimated that at least 60 percent of a population would have to run an app for it to become effective. Others think apps can be modestly helpful even with much smaller adoption rates. But aside from trust issues, the number of people willing to participate seems to have gone down since the first months of the outbreak, as “social distancing fatigue” has set in and public panic over the virus has given way to a more measured caution (and in too many cases, an abandonment of all caution whatsoever).

The bottom line is that there are too few reasons to think that apps will prove more helpful than human memories elicited by experienced contact tracers. The promise of exposure notifications lies in the space between the large pool of incidental contacts that people have, and the smaller number of significant contacts that they remember. The apps promise to track contacts that are close and
sustained enough to pose a serious risk of exposure yet beyond the subject’s memory. For most people, that space may simply not be large enough to be useful.

**Real-World Experiences in States and Other Countries**

Unsurprisingly, given these problems, the states and countries that have experimented with using technology-assisted contact tracing have not met with much success. The use of technology by China and some other Asian countries has received a lot of attention, but as the Minnesota epidemiologists point out, “we don’t know exactly what methods were used, how many cases were involved, and what the estimated impact was in reducing transmission since other mitigation strategies were employed at the same time” in those countries.

That lack of measurement is true throughout the world. An MIT survey of global digital contact-tracing efforts found 43 countries in some stage of offering a product. Ten of those countries are relying on the privacy-preserving Apple/Google protocol, with the rest a jumble of different architectures and policies. It may not be quite true, as UK Prime Minister Boris Johnson declared on June 24, that “No country in the world has a working contact tracing app” — Germany has launched an app that has been downloaded over 14 million times so far, and India claims 131 million downloads for its app and 900,000 users who have been contacted and told to self-isolate. But we don’t know if those numbers represent a high enough proportion of the populations to actually have an impact on slowing the disease in Germany and India, let alone in countries with lower adoption rates. We also don’t know how effective it is to simply tell people to self-isolate, in the absence of social support for them to do so.

It’s also worth noting that in some countries such as China and India, digital tracking is imposed in authoritarian ways that would cause most people who value civil liberties to recoil.

In the U.S., a few states have attempted to launch apps, including Utah, where things went so badly that one program was shut down within 72 hours of its launch, and another one had not led to any contract tracing a month after its launch. An app in North and South Dakota ran into trouble quickly when it was revealed to be sharing data with a private location-data company. Overall, state efforts so far have been plagued by “technical glitches and a general lack of interest by their residents.” A survey by Business Insider found that only three states planned to use the Apple/Google technology. Others had not decided, but 17 states reported that they had no plans to use smartphone-based contact tracing at all.

Those who have worked on privacy-preserving exposure notification apps should be commended for stepping up. They have dedicated their skills toward trying to save lives and restore people’s freedom, and they did a very good job creating a privacy-preserving approach that was not only the most likely to be trusted and effective, but also the least likely to permanently change our world for the worse.

Nevertheless, it does not appear to be working out. “A lot of this is just distraction,” Osterholm
concluded of all the talk over digital contact tracing. “I just don’t see any of this materializing.” Given what we know about the technology, we are inclined to agree.
Civil Rights Groups, Health Advocates and Public Defenders Celebrate Passage of Legislation to Protect Contact Tracing Data from Law Enforcement

Amid Dual Crises of COVID-19 Pandemic & Police Abuse, Advocates Call for Governor Cuomo to Sign the Bill Immediately

July 23, 2020

ALBANY, NY - Today, New York’s legislature passed an essential bill - A.10500-C/S.8450-C - to protect the confidentiality of contact tracing information and prohibit access by law enforcement and immigration enforcement. Sponsored by the chairs of the Senate and Assembly Health Committees, Senator Gustavo Rivera and Assemblymember Richard Gottfried, this bill helps ensure that contact tracing achieves its public health goals and is not weaponized against communities of color.

Contact tracing is a necessary component of the fight against the novel coronavirus. However, participation in contact tracing hinges on public trust. Effective contact tracing requires that participants share a wealth of intimate detail with contact tracers: information about their location, private activities, health status, and associations. If individuals fear that participating in contact tracing will expose them or their loved ones to deportation or criminalization, they will simply choose not to participate. Public health experts know that protecting this intimate information is key to stemming the spread of COVID-19 - and privacy, civil rights, and racial justice advocates agree. Today’s legislation prohibiting law enforcement and immigration enforcement from accessing contact tracing information is integral to achieving public health, privacy, and racial equity.

As COVID-19 contact tracing efforts expand across the state, civil rights groups, health care advocates, immigrants’ rights groups, privacy advocates, and public defenders celebrate the passage of this bill and call for Governor Cuomo to promptly sign it.

Legislators & advocates said the following:

“Contact tracing for COVID-19 is critically important for public health, but it only works if people participate,” said Assembly Health Committee Chair and bill sponsor Richard N. Gottfried. "People need to feel confident that their information will only be used for public health purposes, not as a back door for law enforcement or immigration authorities. It's critical that we put safeguards in place right now, when the program is getting started. I urge the Governor to sign this bill into law as soon as possible."

“Contact tracing is one of our most effective tools to combat COVID-19. However, it will only produce the results we need if the data collected from New Yorkers remains confidential and it is not used for law or immigration enforcement purposes,” said State Senator Gustavo Rivera. "As the Senate sponsor of this bill, I want to thank Assemblymember Gottfried and every advocate who played a critical role in successfully passing this bill. Undoubtedly, this important step will strengthen the public's trust in this program, which will help keep New York on the path to recovery."

Allie Bohm, Policy Counsel for the New York Civil Liberties Union, said: “Information collected to stop a public health emergency has no place in the hands of law enforcement or immigration authorities. As individuals fill the streets protesting for Black lives during a pandemic that is disproportionately killing Black and brown people, law enforcement in Minnesota declared that they would use contact tracing to track protesters. Public health officials immediately lamented that the mere announcement hampered their efforts to build participation in contact tracing as individuals worried that their information would be used to harm their loved ones and contacts. We cannot let that happen here in New York – and passage of A.10500-C/S.8450-C brings us one step closer to making sure it doesn’t. We applaud the legislature for passing this critical legislation and urge Governor Cuomo to immediately sign the bill. It is an action he can take right now that would infuse much-needed trust into New York's contact tracing program and ensure that our recovery efforts do not exacerbate the harms that COVID-19 has already wrought on communities of color."

“There can be no effective contact tracing without trust. We applaud the State Legislature for acting to protect New Yorkers health data, giving contact tracing efforts the best chance to succeed. Black, brown and immigrant communities have not only suffered disproportionately from COVID-19, they continue to be targeted by local law enforcement and ICE. Thanks to the leadership of State Senator Rivera and Assembly Member Gottfried, vulnerable communities can be
Contact tracing confidentiality is necessary to protect the health of our neighbors,” said Alice Fontier, Managing Director of the Neighborhood Defender Service of Harlem. "New Yorkers of color should not have to choose between their health and their privacy. There is no reason that the police or ICE should wield another form of mass surveillance to be weaponized against the communities we serve, particularly at the expense of the health of those vulnerable communities."

"Black communities are bearing the brunt of two pandemics: COVID-19 and police violence,” said Katie Schaffer, Director of Advocacy and Organizing at Center for Community Alternatives. "In our efforts to stop the spread of COVID-19, it is critical that we do not create a new treasure trove of data for law enforcement or immigration enforcement to further target and criminalize communities of color. By passing this legislation, New York’s legislature has demonstrated a commitment to prioritizing public health over criminalization. We call on Governor Cuomo to do the same and sign this bill into law immediately."

"In the midst of an unprecedented public health crisis, our #1 priority should be the health and safety of all New Yorkers," said Scott Levy, Chief Policy Counsel at The Bronx Defenders. "COVID-19 has already caused disproportionate harm to low-income communities of color. The contact tracing process is essential for helping New York recover; it must not be weaponized to target and punish communities that have borne the brunt of this pandemic. Contact tracing is a public health tool, not a tool for law enforcement and ICE. We applaud the Legislature for passing A.10500-C/S.8450-C and urge the Governor to sign it as soon as possible."

"Information collected for COVID-19 contact tracing belongs solely in the hands of public health authorities,” said Jacqueline Seitz, Staff Attorney at the Legal Action Center. "The Gottfried/Rivera bill provides critical privacy safeguards necessary to ensure that all New Yorkers, especially communities of color hardest hit by the pandemic, can provide information to help quell the spread of the disease without fear of law enforcement or immigration repercussions."

"States of emergency have historically provided a ripe opportunity for governments and police to expand their surveillance powers over whoever is considered to be a threat—most recently Black and brown communities, including immigrants—and it is critical that New York State does not allow management of the pandemic to expand the surveillance state,” said Mizue Aizeki, Deputy Director of the Immigrant Defense Project. “We applaud the NYS legislature for ensuring that information provided through contact tracing cannot be weaponized by NYPD, ICE or other policing agencies."

"We are very pleased that the Contact Tracing Confidentially bill has passed in the State Legislature,” said Charles King, CEO and Co-Founder of Housing Works. “COVID-19 is not over; in fact we may see a second wave in the coming months and it is vital that New York State have the best possible contact tracing protocols in place to help reduce and end transmission. Confidentiality will protect New Yorkers from harassment, arrest, detention, or deportation at the hands of ICE or the police, and ensure thorough, useful data as we continue to curtail the spread of this virus. We sincerely hope Governor Cuomo will sign it immediately. Our heartfelt thanks and gratitude go out to the bill’s cosponsors, AM Gottfried and Sen. Rivera, and everyone who helped make this a reality."

"The tracing approach is built upon a basic idea: When someone tests positive for a virus like COVID-19 or becomes sick, you find all the people the infected person came into contact with, because they, too, may be infected. But we have historically seen the pitfalls that occur with tracing when incorporated into the arsenal of racist methods to harm black and brown communities,” said Anthony Feliciano, Director of the Commission on the Public's Health System. “It is not an exaggeration to say that low-income New Yorkers have saved thousands of their neighbors’ lives by allowing them to shelter-in-place. We can honor what many in this case had no other option to go to work by not allowing their safety and well-being to be further harmed. One of the ways is for Bills A10500-C and AS8450-C to be signed by Governor Cuomo immediately. Racism in health care permeates also in the response to the pandemic. The efforts can be embraced by all New Yorkers, if we prevent law enforcement and ICE access and ability to manipulate an important public health measure. It can't be turned into their tool of criminalization and the dehumanizing of Immigrants, Black and other communities of color."

"Contact tracing privacy is not just a civil rights issue, it’s a public health necessity,” said Surveillance Technology Oversight Project Executive Director Albert Fox Cahn. "By passing this measure, New York is leading the national effort to stop contact tracing data from being hijacked by police. We call on Governor Cuomo to sign this vital measure and to reassure all New Yorkers that contact tracing data will never be weaponized by law enforcement. If we fail to act, many of the communities of color that have already suffered the brunt of this pandemic will refuse to cooperate..."
with disease detectives. We also renew our calls for federal protections, holding federal law enforcement agencies to this same standard.”

“Containment of the COVID-19 epidemic hinges on quick identification of those who may be infected and treatment of those who are ill. As the HIV epidemic demonstrated, this is possible only when we insist on a public health response that protects the legitimate privacy concerns of all citizens, particularly those already-marginalized people whom COVID-19 has hit the hardest. The Rivera/Gottfried bill ensures that New York’s response to COVID is grounded in solid public health principles that encourage the trust and participation of all New Yorkers,” said Catherine Hanssens, Founding Executive Director, The Center for HIV Law and Policy.

“COVID19 has taught us the indelible lesson that we are all bound together and are responsible for each other,” said Sarah Chu, Senior Advisor on Forensic Science Policy at the Innocence Project. “When we engage in contact tracing, we are offering data about ourselves, our family members, and our social network with the understanding that it will be used only for our collective public health. A10500-C/S8450-C would formally seal this contract with the power of the law by barring law enforcement from accessing this information. The profound benefits of contact tracing won’t reach the most vulnerable communities, who are already subjected to perpetual surveillance through various criminal justice technologies (facial recognition, gang databases, DNA dragnets), unless we take action now. We thank AM Gottfried and Sen. Rivera for recognizing the urgent and critical need for a bill that will simultaneously protect the health and privacy of all New Yorkers.”

“The Black and brown communities of New York are without question those most directly affected by twin pandemics: the coronavirus and the plague of the surveillance state. This bill rightly adjusts our state-level response to an unparalleled crisis and avoids treating one devastating disease by opening ourselves to another,” said Elizabeth Daniel Vasquez, Special Forensic Science Counsel at Brooklyn Defender Services. “A landmark approach to common-sense goals, this bill ensures that contact-tracing health information remains private and cannot be accessed or weaponized by the police. We call on Governor Cuomo to sign this important legislation immediately.”

"As ICE’s authority continues to grow under a federal administration that is clearly more focused on targeting immigrant communities than COVID-19, trust in government is at an all time low. That’s why it’s imperative that New York State protect the integrity and security of contact tracing data for public good," said Max Hadler, Director of Health Policy at the New York Immigration Coalition. "We call on Governor Cuomo to sign the bill immediately to ensure that the communities hardest hit by COVID-19 can more safely participate in the fight to beat this vicious pandemic and support New York’s recovery."
STATE OF NEW YORK

IN SENATE

June 3, 2020

Introduced by Sens. RIVERA, BAILEY, BENJAMIN, BIAGGI, CARLUCCI, COMRIE, GIANARIS, GOUNARDES, HARCKHAM, HOYLMAN, JACKSON, KAMINSKY, KENNEDY, KRUEGER, LIU, MAY, MYRIE, PARKER, PERSAUD, RAMOS, SALAZAR, SEPULVEDA, SERRANO, STAVISKY, THOMAS -- read twice and ordered printed, and when printed to be committed to the Committee on Health -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the public health law, in relation to the confidentiality of contact tracing information

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Article 21 of the public health law is amended by adding a new title 8 to read as follows:

TITLE 8

NOVEL CORONAVIRUS, COVID-19

Section 2180. Definitions.

2181. COVID-19 contact tracing; confidentiality.

2182. Regulations.

§ 2180. Definitions. As used in this title the following terms shall have the following meanings:

1. "Contact tracing" means case investigation and identification of principal individuals and contact individuals.

2. "Contact tracer" and "contact tracing entity" means an individual or entity employed by or under contract with the state, a local government, a state or local governmental entity, or an agent thereof, to conduct contact tracing, engage in contact tracing, or receive contact tracing information.

3. "Contact tracing information" means any information that includes or can reveal the identity of any principal individual or contact individual, and any COVID-19-related information or test results, received or collected for the purpose or in the course of contact tracing.

EXPLANATION--Matter in italics (underscored) is new; matter in brackets [ ] is old law to be omitted.

LBD16487-14-0
4. "Contact individual" means an individual who has or may have come in contact with a principal individual or who has or may have been exposed to and possibly infected with COVID-19.

5. "Principal individual" means an individual with a confirmed or probable diagnosis of COVID-19.

6. "COVID-19" means infection with or the disease caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2).

7. "Immigration authority" means any entity, officer, employee, or government employee or agent thereof charged with or engaged in enforce- ment of the federal Immigration and Nationality Act, including the United States Immigration and Customs Enforcement or United States Customs and Border Protection, or any successor legislation or entity.

8. "De-identified" means, in relation to contact tracing information, that the information cannot identify or be made to identify or be asso- ciated with a particular individual, directly or indirectly and is subject to technical safeguards and policies and procedures that prevent re-identification, whether intentionally or unintentionally, of any individual.

9. "Law enforcement agent or entity" means any governmental entity or public servant, or agent, contractor or employee thereof, authorized to investigate, prosecute, or make an arrest for a criminal or civil offense, or engaged in any such activity, but shall not mean the depart- ment, the commissioner, a health district, a county department of health, a county health commissioner, a local board of health, a local health officer, the department of health and mental hygiene of the city of New York, or the commissioner of the department of health and mental hygiene of the city of New York.

10. "Support" means resources or services provided to an individual to enable such individual to safely quarantine or isolate, including grocery, meal or pharmacy delivery, laundry services, child or elder care, pet walking, assistance with telephone, internet, or other commu- nication services or devices, health and mental health services, legal services, provision of appropriate living space for individuals who cannot isolate or quarantine at home, and income replacement. "Support" may also include support provided to other individuals for whom the individual commonly provides those resources or services.

11. "Permitted purpose" means:
   (a) disclosure to appropriate health care providers or their personnel for the purpose of the clinical diagnosis, care or treatment of the principal individual or contact individual who is the subject of the information, where an emergency exists and the individual is in immedi- ate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the indi- vidual’s life or health;
   (b) facilitating a legally-authorized public health-related action, in relation to a specified principal individual or contact individual, where and only to the extent necessary to protect the public health; or
   (c) the investigation, prosecution or defense of a civil or legal action for a violation of this title; provided that if the use is initi- ated by a party other than the principal individual or contact individ- ual who is the subject of the contact tracing information, the informa- tion must be highly material and relevant for the purpose.

§ 2181. COVID-19 contact tracing; confidentiality. 1. (a) All contact tracing information shall be kept confidential by any contact tracer and contact tracing entity, and may not be disclosed except as necessary to carry out contact tracing or a permitted purpose.
Where a contact tracer or contact tracing entity discloses contact tracing information for a permitted purpose, the contact tracer or contact tracing entity shall make a record of the disclosure, including to whom it was made, which shall be part of the contact tracing information.

2. (a) An individual may waive the confidentiality provided for by this section, only by a written, informed and voluntary waiver, in plain language and in a language understandable to the individual making the waiver, and not part of any other document. The waiver shall state the scope and limit of the waiver. If an individual lacks the capacity to make a waiver, an individual authorized to consent to health care for the individual, or the individual's legal representative, may make the waiver. However, a waiver of confidentiality is not required to be written if it is solely for the purpose of arranging or providing support for the individual who is the subject of the contact tracing information.

(b) A waiver of confidentiality under this section shall only apply for the purpose of arranging or providing support if the individual who is the subject of the contact tracing information provides voluntary informed consent to the arranging or providing of the support.

3. A disclosure of contact tracing information authorized under this section shall be limited in scope as to the identity of any individual, the information to be disclosed, and the party to which disclosure may be made, and as necessary to achieve the purpose of the disclosure under this section, and shall not authorize re-disclosure except as explicitly authorized by the terms of the waiver under this section. However, this section does not bar disclosure of contact tracing information pertaining to and identifying a principal individual or contact individual by the individual who is identified.

4. (a) This section does not bar otherwise-lawful disclosure, possession or use of contact tracing information, including aggregate contact tracing information, that is de-identified. Disclosure, possession or use under this subdivision shall only be for a public health or public health research purpose.

(b) A person or entity may only possess or use de-identified contact tracing information if the person or entity maintains technical safeguards and policies and procedures that prevent re-identification, whether intentional or unintentional, of any individual, as may be required by the commissioner (or the New York city commissioner of health and mental hygiene in the case of contact tracing information collected by or under authority of the New York city department of health and mental hygiene or the New York city health and hospitals corporation). The commissioner (or the New York city commissioner as the case may be) shall require safeguards, policies and procedures under this paragraph as the commissioner deems practicable.

(c) Disclosure, possession and use of de-identified contact tracing information under this subdivision shall be only pursuant to approval by the commissioner (or the New York city commissioner of health and mental hygiene in the case of contact tracing information collected by or under authority of the New York city department of health and mental hygiene or the New York city health and hospitals corporation) specifying the purpose, nature and scope of the disclosure, possession and use and measures to ensure that it will comply with this section and the terms of the approval.

5. No law enforcement agent or entity or immigration authority shall be a contact tracer or contact tracing entity or engage in contact trac-
This subdivision does not bar an individual who is associated with a law enforcement entity or immigration authority from acting only as a principal individual or contact individual.

6. No contact tracer or contact tracing entity may provide contact tracing information to a law enforcement agent or entity or immigration authority. Without consent under subdivision two of this section, contact tracing information and any evidence derived therefrom shall not be subject to or provided in response to any legal process or be admissible for any purpose in any judicial or administrative action or proceeding. However, this subdivision does not restrict providing information, relating to a specified principal individual or contact individual, where and only to the extent necessary for a permitted purpose.

7. (a) The commissioner (or the New York city commissioner of health and mental hygiene in the case of contact tracing information collected by or under authority of the New York city department of health and mental hygiene or the New York city health and hospitals corporation) shall make regulations to require that contact tracing information possessed, used or under the control of a contact tracer or contact tracing entity shall be subject to technical safeguards and policies and procedures for storage, transmission, use and protection of the information. The regulations shall prevent possession, use or disclosure of the contact tracing information not permitted by this title, and shall be at least as or more protective than the safeguards, policies and procedures the commissioner (or the New York city commissioner as the case may be) provides for other confidential information.

(b) This paragraph applies where contact tracing information is possessed or controlled by a contact tracer or contact tracing entity that is a non-governmental individual or entity employed by or under contract with a governmental entity, or an agent thereof. Within thirty days of collecting or receiving the contact tracing information, the non-governmental individual or entity shall (i) remove information from its possession or control and deliver it to the appropriate governmental contact tracing entity, retaining no copy of it; (ii) expunge the information from its possession or control; or (iii) de-identify the information. However, the expungement or de-identification of particular contact tracing information may be postponed for up to fifteen days while the contact tracer or contact tracing entity is actively engaged in contact tracing using that information, provided that the principal individual or contact individual to whom it pertains gives voluntary informed consent. The disclosure, possession and use of the de-identified contact tracing information shall be subject to subdivision four of this section.

§ 2182. Regulations. The commissioner shall make regulations implementing this title.

§ 2. This act shall take effect immediately.
Masks and Face Coverings: What Employers Need to Know

By Alka Ramchandani-Raj and Devjani H. Mishra on April 13, 2020

NOTE: Because the COVID-19 situation and response are dynamic, with new governmental measures each day, employers should consult with counsel for the latest developments and updated guidance on this topic.

On April 12, 2020, New York State became the latest and largest jurisdiction to impose face-covering requirements in response to the ongoing COVID-19 pandemic. Governor Andrew Cuomo issued an executive order requiring “all essential businesses or entities” to provide “any employees who are present in the workplace” with face coverings to wear “when in direct contact with customers or members of the public,” and specifying that businesses “must provide” such face coverings “at their expense.” This order becomes effective Wednesday, April 15 at 8 p.m.¹

New York thus joins New Jersey, the District of Columbia, Los Angeles City and County, Miami-Dade County and numerous other localities in requiring or recommending the use of masks or other face coverings in the workplace and elsewhere in public. This trend is expected to continue in light of evolving recommendations from the Centers for Disease Control and Prevention (CDC).

The following are answers to some of the most common employer questions in this developing area.

What is a “mask,” and what is a “face covering”?

In interpreting these orders, it is important to distinguish between different types of masks and face coverings.

A mask is usually defined in workspaces as either (i) a filtering respirator such as an N95 or K95 or (ii) a specialized medical grade or surgical mask. Given continuing shortages and supply challenges, both types of masks should generally be reserved for health care providers, first responders and essential workers who need to fulfill task-specific OSHA and workplace safety requirements related to respiratory protection. As manufacturing ramps up, surgical masks may become more easily obtainable by employers in large quantities, and they typically would meet the requirements of the various orders that have issued to date, but priority should be given to the health care and first responder systems.

In contrast, a face covering is a cloth, bandana, or other type of material that covers an employee’s mouth and nose. The CDC lists five criteria for “cloth face coverings,” which should:

- fit snugly but comfortably against the side of the face
- be secured with ties or ear loops
- include multiple layers of fabric
- allow for breathing without restriction
be able to be laundered and machine-dried without damage or change to shape.

Other types of improvised coverings, such as a scarf or single cloth layer that does not meet the above criteria, would not be adequate under most orders mandating face covering. Single-use paper-based face coverings may be an option, but their effectiveness varies and the CDC has not issued any specific recommendations with regard to their use. Other types of specialty or industrial coverings (e.g., barrier full-face shields) should be reserved for their normal uses and employers are not expected to make these available to workers who would not regularly be using them.

I thought we weren’t supposed to wear masks or face coverings – what changed?

Through March, the CDC and other U.S. authorities were not recommending the widespread use of face coverings. On April 3, 2020, however, the CDC changed its prior guidance, recommending that individuals should wear cloth face coverings in public settings where social distancing measures and other hygiene practices are difficult to maintain. On April 9, 2020, the CDC amplified this guidance with respect to “essential employees” (generally, those who have been exempted from stay-home or shelter-in-place orders) who may have been exposed to COVID-19, recommending that such employees wear face coverings at all times while in the workplace for at least 14 days, in addition to other precautionary measures.

Does a face covering prevent the wearer from contracting COVID-19?

A face covering is not necessarily meant to protect the wearer from others. Rather, the intention is to prevent a possibly asymptomatic person from unknowingly transmitting the virus to others. As the CDC has cautioned, face coverings are just one protective measure, and not a substitute for social distancing, personal hygiene, and additional cleaning protocols.

In general, where an employer becomes aware that a worker is actively symptomatic for COVID-19, steps should be taken to exclude that worker from the workplace as well as to identify others who may have been exposed, and to develop an appropriate return-to-work plan when the worker’s symptoms have resolved. Note that under the Los Angeles City Order, and according to CDC guidance, employees of essential services and businesses who are COVID-19 positive but remain asymptomatic and are able to work may do so with face coverings and assuming that other protective measures are being taken.

Who pays for face coverings?

New York specifically requires employers to provide employees in essential, customer-facing roles with face coverings at the employer’s expense. Similarly, New Jersey requires restaurants, dining establishments and other food service businesses, as well as various public employers, to provide their employees with face coverings and gloves at the business’s expense. Other jurisdictions, such as Los Angeles, do not specify who should provide or pay for face coverings.

However, the employer may have that obligation under general state or local laws obligating employers to provide or pay for equipment like face coverings. As noted, Governor Cuomo’s Order specifically requires employers to pay for face coverings for essential, customer-facing employees. In contrast, OSHA and the DOL have not provided guidance whether face coverings must be provided or paid for by the employer. In other states, employers should review wage and hour and workplace safety regulations to determine if they are obligated to pay for face coverings and other items recommended for COVID-19 protection.

What about training?
Employers should provide employees with instructions and/or training on how to wear, maintain and clean their face coverings. Employees need to know that they must securely cover their noses and mouths, should not reverse, move or remove their face coverings unnecessarily in the workplace, should not share their face coverings with others, and must keep them clean.

Single-use face coverings must be properly and safely discarded into trash receptacles after each use. Employers that opt to provide employees with single-use coverings must provide a sufficient supply to enable employees to replace them as needed, which may be more than once a day.

**Who does the cleaning and maintenance, and who pays for it?**

As the CDC states, multiple-use face coverings should “be able to be laundered and machine dried without damage or change to shape,” generally at least once a day (as the Los Angeles City Order specifies) or more often if contamination occurs. Regardless of whether face coverings are governmentally mandated, required by employer policy, or merely recommended, proper cleaning and maintenance are critical to ensure that employees do not reuse dirty or contaminated face coverings, which pose a hazard to other employees as well as customers.

In principle, responsibility for cleaning expenses could vary based on state uniform maintenance rules. For example, under New York State's Minimum Wage Orders, most employers have the option to either launder uniforms or to pay the employee a set premium to cover cleaning expenses. In contrast, hospitality employers in New York may apply a “wash and wear” exception for items that can be routinely washed along with an employee’s ordinary clothes, and do not have to pay the employee a premium. An employer seeking to rely on this exception will need to furnish an employee with a sufficient number of face coverings to correspond to the employee’s full workweek, noting that face coverings may need to be changed more than once a day, and will need to supply face coverings that will not be damaged by normal laundering.

In the absence of a wash and wear exception, or if there are questions about whether employees will be able to manage regular maintenance, employers are strongly advised to either provide employees with a cleaning subsidy or set up an in-house cleaning program at the employer’s expense. In the latter case, employees should understand that they may not get their own face coverings back after cleaning, and may need to carry additional coverings with them to wear during their commute home. Whatever approach employers take, they must ensure that their program complies with all locally applicable wage and hour requirements.

**Where can employers obtain face coverings for their employees? What should employers do if they cannot obtain them?**

This is perhaps the most pressing question related to face coverings, and the least easily answered given ongoing shortages of protective equipment. Where states and localities are mandating face coverings, employers should be making and documenting good-faith efforts to secure face coverings as a required element of doing business.

The CDC’s website includes do-it-yourself (DIY) options for making one’s own face covering using materials such as T-shirts, bandanas, and hair ties, and numerous similar tutorials can be found online. Employers should consider providing employees with such instructions and materials (at the employer’s expense) as an interim measure while they continue to source more standard face coverings. In such cases, the employee’s time spent making face coverings is likely to be compensable and the employer should factor that expense into its planning.

**What if employees want to use their own face coverings?**
This may be a good option where the employer is having difficulty sourcing face coverings. Employees who are using their own face coverings must make sure that these coverings meet the CDC’s recommendations and that they clean them correctly. Employers should provide employees a reimbursement or subsidy for material and cleaning costs. Given the proliferation of novelty masks and materials, employees should be cautioned that DIY face coverings must be workplace-appropriate and cannot feature offensive images or content.

**What if an employer has distributed face coverings, but an employee fails to bring their face covering to work?**

Because face coverings are considered protective equipment, the employee should not be permitted to work on-site until they are able to obtain a face covering.

**What if an employee declines to wear a face covering for medical reasons?**

Generally, employers should be providing training to employees at the time that face coverings are distributed or implemented, and the training process should include identification of any medical issues that could interfere with wearing face coverings, such as claustrophobia, asthma, COPD or other conditions. Employers are advised to engage in the interactive process with such employees as required by the Americans with Disabilities Act (ADA) and similar state and local provisions. An employee who cannot breathe through a face covering should not be required to wear one, but may need to be temporarily removed from customer-facing responsibilities, provided with leave or accommodated in some other fashion.

**What if an employee declines to wear a face covering for non-medical reasons?**

Employee objections should be evaluated in light of all of the relevant circumstances. For example, an employee may raise objections based on religious grounds, where their pre-existing grooming or dress requirements conflict or interfere with prescribed face coverings. In such cases, the employer should engage in the interactive process as required by Title VII and similar state and local provisions.

Individuals have also raised legitimate bias concerns, such as where people of color wearing face coverings are wrongly suspected of criminal intent and activity. Employers should take steps to minimize this risk by sourcing face coverings that more clearly look like protective masks and by posting notices that employees are required to wear face coverings on site.

Individuals may also object based on the fact that a face covering interferes with their ability to perform the job. Again, employers should assess this issue during the rollout process, identify cases where face coverings may inhibit job performance and develop workarounds that do not compromise safety or performance.

Individuals who simply decline to wear face coverings, but do not raise a medical or otherwise protected objection, should not be permitted to work and may be disciplined for not following work requirements.

**What are the penalties for non-compliance?**

States and localities are imposing a variety of penalties for non-compliance, and local police are generally tasked with enforcement. In New Jersey, non-compliance will be prosecuted as disorderly conduct. In the City of Los Angeles, failure to comply constitutes a misdemeanor subject to fines and/or imprisonment. In New York, fines and penalties may be imposed for violation of the Public Health Law.

**What’s next?**
Face covering requirements are expanding, and are likely to remain in place for the next several months. The CDC has also recommended face covering as a protective measure for returning essential employees to work following COVID-19 exposure. As such, employers should make reasonable efforts to source face coverings for essential workers, particularly those who interface with customers and others, and consider what other safety measures may be needed as employees transition back to on-site work in greater numbers.

1 On April 15, 2020, Governor Cuomo issued an additional executive order requiring members of the public to wear face coverings whenever they are unable to maintain social distancing, effective April 17. However, this April 15 order does not impose specific requirements on employers to supply or pay for such face coverings.

2 Minimum Wage Order for Miscellaneous Industries and Occupations, 12 N.Y.C.R.R Part 142-2.5(c).

3 Hospitality Industry Minimum Wage Order, 12 N.Y.C.R.R. Part 146-1.7(b).

Information contained in this publication is intended for informational purposes only and does not constitute legal advice or opinion, nor is it a substitute for the professional judgment of an attorney.

By Zoe Argento, Philip Gordon, Kwabena Appenteng, and Anna Park on August 3, 2020

With the resurgence of COVID-19 infections across the United States, employers are facing growing pressure to ascertain whether their employees have contracted the virus. Temperature checks and symptoms screening, while helpful, will not identify employees who are asymptomatic and potentially contagious. This gap is critical because studies show that up to 45% of people infected with the virus do not show any symptoms. As a result, COVID-19 testing can be essential to remaining operational or reopening after a workplace outbreak.

The Equal Employment Opportunity Commission (EEOC) has issued guidance stating that mandatory testing of employees for COVID-19 falls within an exception to the Americans with Disabilities Act's (ADA) general prohibition against mandatory medical examinations of employees. While lawful under the ADA, testing presents serious privacy and information security risks for employers. We describe in this article the common concerns raised at each stage of the testing process, from deciding whom to test to handling the test results. For each stage, we describe practical steps employers can take to help address these concerns.

Who Should be Tested and How Frequently: Reducing the Risk of Unlawful Data Collection

In deciding which employees to test and how frequently to test them, employers must tailor their testing program to align with the rationale for legally permissible testing. Although the ADA generally prohibits medical examinations of employees, such examinations are permissible to determine whether an employee poses a direct threat to the workplace. In guidance issued on April 23, 2020, the EEOC clarified that the COVID-19 pandemic poses a direct threat to the workplace, opening the door for COVID-19 testing of employees to reduce the risk of infection of co-workers and others. That guidance, however, does not mean employers necessarily could justify the substantial privacy intrusion of frequent testing of all employees.

To help minimize intrusiveness and ensure that COVID-19 testing will fall within the “direct threat exception” to the ADA's general prohibition on employee testing, employers should design their testing program based on objective evidence of how the virus spreads and how the test detects the virus. For example, testing employees who work exclusively in their own office where they can isolate themselves from co-workers may be more difficult to justify than testing factory workers who cannot engage in social distancing because of the nature of the manufacturing process. As another example, testing employees who must engage in business travel to perform their job responsibilities generally should be delayed until a few days after those employees have completed business travel (assuming they are asymptomatic at that
time) because studies indicate that individuals may not have reliably detectable levels of virus until several days after exposure. Consequently, testing these employees on the day they return from business travel would more likely result in false negatives and arguably would not be necessary to prevent a direct threat to the workplace.

As these examples highlight, employers need to design their testing program to ensure that the testing at least has the potential to materially reduce the risk of COVID-19 infection in the workplace. Therefore, when structuring the program, employers should evaluate a wide range of factors specific to the employer’s workplace, such as where and how employees perform their job responsibilities, the nature of the business, the physical layout of the workplace, and the degree of community spread in the relevant jurisdiction. The results of this evaluation should serve as the basis for a written testing protocol. Adherence to the protocol would assist the employer to conduct testing in a consistent manner across the organization. In addition, the protocol would support the conclusion that the employer conducts COVID-19 testing only as necessary to prevent a direct threat to the workplace. Of course, any testing protocol will need to be administered across similarly situated employees to avoid allegations of discrimination. At the same time, employers should permit limited exceptions as necessary to accommodate disabled employees and employees’ religious beliefs.

Selecting the Test: Accuracy and Reliability

Due to the inherent invasiveness of medical examinations, employers should avoid subjecting employees to COVID-19 tests unless they provide useful results. Indeed, the EEOC’s guidance emphasizes that only “accurate and reliable” COVID-19 tests fall within the “direct threat exception” to the ADA’s general prohibition on employee testing. Consequently, employers’ test selection is fundamental to the lawfulness of the testing program.

COVID-19 tests currently fall into the following three high-level categories with varying levels of accuracy and reliability:

1. **Virus tests**: tests for the presence of the SARS-CoV-2 virus that causes COVID-19;
2. **Antibody tests**: tests for antibodies to the virus; and
3. **Antigen tests**: tests for the presence of proteins that are part of the virus.

Of these, the most likely candidate for employers is the virus test. In guidance issued on June 17, 2020, the EEOC opined that the ADA does not permit antibody tests. The EEOC cited the Centers for Disease Control and Prevention’s (CDC) own guidance that antibody tests “should not be used to make decisions about returning persons to the workplace,” because they are not sufficiently accurate or reliable. Also, at least at this time, antigen tests show low levels of accuracy compared to tests for the virus itself and, therefore, also are likely impermissible under the ADA.

Even when selecting a virus test, employers need to confirm the test’s reliability. For example, while many “rapid” testing products are making their way into the marketplace, their accuracy and reliability may be subject to challenge.

How to Conduct COVID-19 Testing in Compliance with HIPAA, the ADA, and the CCPA

The Health Insurance Portability and Accountability Act (HIPAA) and the ADA closely regulate the collection, use and disclosure of health data, and the California Consumer Privacy Act (CCPA) establishes notice requirements for the collection of any type of employee personal information. To lawfully obtain and use the results of employees’ COVID-19 tests, employers must structure the testing process to comply with these laws.

**HIPAA Considerations**
Regardless of whether an employer relies on in-house medical staff, a third-party service provider, or employees themselves to collect the specimen for COVID-19 testing, most employers will have no choice but to rely on a third-party laboratory to test the specimen for the presence of COVID-19. Many testing laboratories are “covered entities” subject to HIPAA. When a HIPAA-covered laboratory conducts the COVID-19 test, the test results and all related health and demographic information are protected health information (PHI) that must be handled in compliance with HIPAA.

HIPAA generally prohibits a covered entity from disclosing PHI without the subject’s first executing a HIPAA-compliant authorization. That means testing laboratories subject to HIPAA cannot disclose COVID-19 test results to the employer without a HIPAA-compliant authorization executed by the employee. Several states add state-specific requirements to the contents of this authorization form. Employers should, therefore, include in their employee-testing packet a HIPAA-compliant authorization form that employees must sign and provide to the testing laboratory when the testing laboratory is subject to HIPAA.

Some testing laboratories are not subject to HIPAA. Using such laboratories would avoid the need to obtain a HIPAA-compliant authorization from each employee who is tested. That benefit generally will not outweigh two key advantages of using a HIPAA-covered testing lab. First, HIPAA-covered labs are required to implement the extensive information security safeguards required by the HIPAA Security Rule, thereby reducing the risk of a security breach (discussed further below) involving COVID-19 test results. Second, employees may have a greater level of trust in a HIPAA-covered testing lab and be less likely to refuse to participate in the testing program.

**ADA Considerations**

Once the employer receives the COVID-19 test results, the employer must handle them in compliance with the ADA — regardless of whether the testing laboratory is subject to HIPAA. The ADA applies to any employee health information received by an employer when assessing whether employees constitute a direct threat to the workplace, i.e., are infected by COVID-19.

The ADA requires employers to maintain the confidentiality of the results of employee medical examinations. In particular, the test results must be maintained in a confidential medical file separate from the general personnel file. Only those employees who need the test outcome to protect the workplace from COVID-19 infection should be granted access to the information. For many employers, this means a small group of employees, typically including HR professionals, who are responsible for the organization’s COVID-19 response.

The ADA also prohibits employers from disclosing employee medical information to third parties except in narrow circumstances that generally will not apply in the context of COVID-19 testing. Consequently, those employees authorized to review test results should be trained not to disclose them to third parties with one important exception. The EEOC has issued guidance stating that employers may disclose positive COVID-19 test results to relevant public health authorities.

The ADA raises one other noteworthy consideration. The ADA allows employers to conduct voluntary medical examinations only as part of an “employee health program.” Such programs must comply with several regulatory requirements, including (a) a prohibition on disclosure to the employer of employee medical information gathered through the program, and (b) distribution of a notice to employees that informs employees, among other things, of the confidentiality requirement. To complicate matters further, in certain conditions, an “employee health program” that offers voluntary COVID-19 testing will be subject to ERISA. As a result of these requirements, voluntary COVID-19 testing may not be an attractive option for many employers.

**CCPA Notice Requirements**
The CCPA requires covered employers to provide employees who reside in California with a “notice at collection” at or before the point when the employer obtains the test results. This notice must describe the categories of personal information to be collected and how the employer will use the information. Generally, employers will find it most convenient to provide the notice either as part of a general announcement of the testing program or when the specimen is collected (unless the employee engages in self-collection). The employer must then use the test results only for the purposes detailed in the notice and ensure that the testing lab does the same.

**Safeguarding Test Results to Reduce Data Security Risks**

Employers need to protect against a security breach involving COVID-19 test results in their own possession. In many states, the unauthorized acquisition of health data may constitute a data breach. Nineteen states, the District of Columbia and Puerto Rico define health information as “personal information” for purposes of data breach notification laws. In these states, a breach of COVID-19 test results — whether positive or negative — might require notifications to the affected employees and, in some states, to government authorities.

The security breach risk is especially high for employers in California, which is one of the states that classifies health information as “personal information” for purposes of data breach notification laws. Under the CCPA, California residents now have the right to recover up to $750 in statutory damages for a breach of health data, on an individual or class-wide basis, when that breach results from the employer’s failure to implement reasonable safeguards for the compromised information.

Employers also should consider the risk of a security breach when contracting with testing laboratories. If the testing laboratory is subject to HIPAA and employees’ test results are compromised, the laboratory would be required to notify relevant employees and the U.S. Department of Health and Human Services of the security breach. Although the laboratory would bear the brunt of the cost, the employer likely would incur costs itself and be confronted with employee complaints. Consequently, employers should ensure that any agreement with a testing laboratory, at a minimum, impose stringent information security standards on the laboratory and address the risks associated with a security breach. Even when the testing laboratory is not subject to HIPAA, employers should consider obtaining similar provisions in the service agreement because, as described above, many state data breach notification laws require notification when health information is compromised.

**Takeaways**

Employers planning to test their employees for COVID-19 should consider taking the following steps:

- Implement a protocol that aligns the scope and frequency of testing with the objective of reducing the direct threat of COVID-19 infection to the workplace;
- Select an accurate and reliable COVID-19 test;
- Inform employees of the testing program and provide a CCPA notice at collection when applicable;
- Require employees to execute a HIPAA-compliant authorization to allow any HIPAA-covered testing laboratory to disclose the COVID-19 test results to the employer;
- Implement safeguards for test results that are maintained by the employer; and
- Include in the service agreement with any testing laboratory provisions that address information security and the risk of a security breach.

2 Lauren M. Kucirka, et al., Variation in False-Negative Rate of Reverse Transcriptase Polymerase Chain Reaction–Based SARS-CoV-2 Tests by Time Since Exposure, Annals of Internal Medicine, May 13, 2020.


Information contained in this publication is intended for informational purposes only and does not constitute legal advice or opinion, nor is it a substitute for the professional judgment of an attorney.

© 2020 Littler Mendelson P.C.
Littler Mendelson is part of the international legal practice Littler Global which operates worldwide through a number of separate legal entities. Attorney Advertising.
This Won’t Hurt a Bit: Employee Temperature and Health Screenings – A List of Statewide Orders

By Littler Mendelson on September 8, 2020

Governors and public health officials across the country have implemented stringent measures to help contain the spread of COVID-19, such as safer at home and face covering mandates. Some jurisdictions also require employers to screen the health of employees, often as they begin a shift. These health screening steps, including temperature checks, have become more common as states reopen their economies.

This post, current as of September 8, 2020 at 8:00 a.m. (CDT), covers statewide laws and orders that require employers to take employees' temperatures and/or conduct other employee health screening procedures, such as asking employees about any COVID-19-consistent symptoms using a questionnaire or checklist. This chart covers only generally applicable requirements and does not cover the heightened requirements applicable to certain types of employees, such as healthcare workers; public health workers; long-term care, assisted living, and nursing home workers; first responders; and law enforcement. We will update this list regularly but expect it will become outdated quickly as new announcements are made.

Note that this list does not include temperature or health screening requirements at the local level. If you would like more information, please contact your Littler attorney for additional resources that summarize such requirements at both the state and local level.

In addition, this post does not address other significant issues related to employer screenings of employee health, including potential wage and hour, discrimination, and privacy concerns. As a result, employers should consult with counsel for details on additional orders that may apply to their operations and for guidance on related legal questions.

Tracking and complying with these requirements present significant challenges for employers, particularly those operating in different locations around the country. To assist our clients with these challenges, our ComplianceHR has created SmartScreen™, an automated screening solution that allows employers to easily send jurisdiction-specific screening questionnaires for select employees to complete before they come into the office each day. Please visit https://compliancehr.com/solutions/smartscreen/ for more information about this solution, or contact info@compliancehr.com to set up a demo.

Employers interested in further information may wish to consult our articles identifying face covering guidance and return to work protocols, as well as our interactive reopening map.

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Temperature Screening</th>
<th>Other Health Screening</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Temperature Screening</th>
<th>Other Health Screening</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alabama</strong></td>
<td>Recommended. <em>Best practice</em>: employers should take temperatures onsite with a no-touch thermometer each day upon a person's arrival at work. <em>Minimum practice</em>: an employee may take his or her temperature before arriving. In either case, a normal temperature does not exceed 100.4F.</td>
<td>Recommended. Employers should screen all employees reporting to work for COVID-19 symptoms with specified questions.</td>
</tr>
</tbody>
</table>
| **Alaska**   | No requirement | Recommended. Reopening businesses should conduct pre-shift symptom screening  

**NOTE:** At least one Alaska locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction. |
| **Arizona**  | Required for restaurants, bars, nightclubs, gyms, fitness centers, indoor theaters, and water parks/tubing facilities. Employers must conduct wellness/symptom checks, including temperature checks for all personnel, at the door and before the opening of the establishment. Health checks are recommended for all other businesses. | Required for restaurants, bars, nightclubs, gyms, fitness centers, indoor theaters, and water parks/tubing facilities. Employers must conduct wellness/symptom checks, including temperature checks for all personnel, at the door and before the opening of the establishment. Health checks are recommended for all other businesses. |
| **Arkansas** | No requirement | Required for restaurant employers. All staff shall be screened for specified symptoms daily before entering the workplace.  

**Required** for gyms and fitness centers. All staff shall be screened for specified symptoms daily before entering the workplace.  

**Recommended generally.** Employees should be screened for fever, cough, shortness of breath, sore throat, or loss of taste or smell as they are entering the building at the beginning work. |
<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Temperature Screening</th>
<th>Other Health Screening</th>
</tr>
</thead>
<tbody>
<tr>
<td>California</td>
<td>No requirement.</td>
<td>Required. Employers must train employees on how to limit the spread of COVID-19, including how to screen themselves for symptoms and stay home if they have them.</td>
</tr>
</tbody>
</table>
<pre><code>                                                             | NOTE: Some California localities have provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction. |
                                                             | Required. Employers must train employees on how to limit the spread of COVID-19, including how to screen themselves for symptoms and stay home if they have them. |
                                                             | NOTE: Some California localities have provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction. |
</code></pre>
<p>| Colorado      | Required. Employers must conduct daily temperature checks at the worksite to the greatest extent possible, or if not practicable, through self-assessment at home prior to coming to the worksite. State guidance provides that all information about employee illness must be treated as a confidential medical record. | Required. Employers must implement daily symptom monitoring protocols at the worksite to the greatest extent possible, or if not practicable, through self-assessment at home prior to coming to the worksite. Employers may use an employee health screening form for checking symptoms. State guidance provides that all information about employee illness must be treated as a confidential medical record |
| Employers with over 50 employees in any one location shall, in addition to the above requirements, implement employee screening systems that follow the above requirements in one of the following ways: (1) set up stations at the worksite for symptom screening and temperature checks; or (2) create a business policy that requires at-home employee self-screening each work day and reporting of the results to the employer prior to entering the worksite. |
| NOTE: Some Colorado localities have provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction. |</p>
<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Temperature Screening</th>
<th>Other Health Screening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecticut</td>
<td>Recommended. Employees should take their temperature before they go to work. If they have a temperature above 100.4F, they should stay home.</td>
<td>Required for personal care services, retail, restaurants, and office-based businesses. These employers must ask employees resuming on-premises work to confirm they have not experienced COVID-19 CDC-defined symptoms and to monitor their own symptoms, including cough, shortness of breath, or any two of the additional symptoms enumerated in the guidance.</td>
</tr>
<tr>
<td>Delaware</td>
<td>Required for high-risk businesses and recommended for all others: each employee must be asked about and report body temperature at or above 99.5F. If a facility has the capability to perform active temperature monitoring, they may do so.</td>
<td>Required for high-risk businesses and recommended for all others: employers must screen each incoming employee with a basic questionnaire. Division of Public Health Essential Services Screening Policy. <strong>NOTE:</strong> At least one Delaware locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>No requirement</td>
<td>Required. Retail food sellers (including grocery stores, supermarkets, convenience stores, food halls, and food banks) must check employees for symptoms before their shifts and exclude employees with cold- or flu-like symptoms. If an employee exhibits symptoms during shift, exclude that employee. <strong>Recommended</strong> for restaurants: screen employees by assessing symptoms of workers (including fever) with a questionnaire, at the beginning of their shift, ideally before entering the facility or operation.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Florida</td>
<td>No requirement</td>
<td>Required for restaurants and food establishments. Managers/supervisors shall meet each employee outside the establishment upon an employee’s arrival for a work shift. The manager shall evaluate the employee for obvious signs of illness and send the employee home if symptoms such as cough, fever, shortness of breath, sore throat, or signs of a respiratory infection are directly observed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: At least one Florida locality has provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Georgia</td>
<td>No requirement</td>
<td>Required for restaurants, bars, and all other non-critical businesses conducting in-person operations. Employers must screen and evaluate employees who exhibit signs of illness, such as a fever over 100.4F, cough, or shortness of breath. Employers must require employees who exhibit signs of illness to seek medical attention and not report to work.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Strongly recommended for all other businesses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gyms and fitness centers are also required to screen patrons at entrance and refuse entry to those displaying symptoms.</td>
</tr>
<tr>
<td>Hawaii</td>
<td>No requirement</td>
<td>No requirement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: At least one Hawaii locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>Idaho</strong></td>
<td>Restaurant employers, personal care services, and gyms and fitness centers should check temperature with non-contact thermometer; if no fever, which is a temperature greater than 100.4°F, or COVID-19 symptoms are present, require workers to self-monitor and report onset of symptoms during their shift. <strong>NOTE:</strong> At least one Idaho locality has provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
<td>Restaurant employers, personal care services, and gyms and fitness centers should monitor employee health by screening employees for fever and symptoms before every shift. <strong>NOTE:</strong> At least one Idaho locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td><strong>Illinois</strong></td>
<td>Recommended for specified employers: Employers should make temperature checks available for employees and encourage their use.</td>
<td>Recommended for specified employers: Employer should conduct in-person screening of employees upon entry into workplace and mid-shift screening to verify no presence of COVID-19 symptoms. <strong>NOTE:</strong> At least one Illinois locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td><strong>Indiana</strong></td>
<td>Recommended for reopening businesses but not required.</td>
<td><strong>Required</strong>. Reopening businesses must conduct employee health screenings. <strong>Required</strong> for food industry workers. <strong>NOTE:</strong> At least one Indiana locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Iowa</td>
<td>No requirement</td>
<td><strong>Recommended</strong> for personal care services employers: ask employees and the public to acknowledge upon entry that they do not currently have symptoms and that they have not been around anyone with a confirmed COVID-19 diagnosis in the last 14 days.</td>
</tr>
<tr>
<td>Kansas</td>
<td><strong>Recommended</strong>. Employers should monitor employees’ temperatures regularly. The state provides a <a href="#">template screening form</a> for logging symptoms. <strong>NOTE</strong>: At least one Kansas locality has provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
<td><strong>Recommended</strong>. Employers should monitor employees’ symptoms regularly. The state provides a <a href="#">template screening form</a> for logging symptoms. <strong>NOTE</strong>: At least one Kansas locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Kentucky</td>
<td><strong>Required</strong>. All businesses, including those that were permitted to remain open, must require employees to undergo daily temperature checks. Businesses may choose whether to require (1) on-site temperature screenings, or (2) self-screenings conducted by employees at home at least once every 24 hours, ideally just before going to work, and reported to the employer prior to beginning work. Employees with a fever above 100.4° should not report to work.</td>
<td><strong>Required</strong>. All businesses, including those that were permitted to remain open, must require employees to undergo daily health assessments for specified symptoms. These assessments may be either self-administered or administered by the business prior to workplace entry. Self-administered assessments may performed at home. <strong>NOTE</strong>: At least one Kentucky locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Louisiana</td>
<td>No requirement</td>
<td>Recommended. Employees who appear to have acute respiratory illness symptoms upon arrival to work should be separated from other employees and sent home.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> At least one Louisiana locality has provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
<td><strong>NOTE:</strong> At least one Louisiana locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Maine</td>
<td>No requirement</td>
<td>No requirement</td>
</tr>
<tr>
<td>Maryland</td>
<td>Recommended. Employers should implement a daily screening process for workers and other personnel which include CDC or MDH recommended health questions and consider temperature testing.</td>
<td>Recommended. Employers should implement a daily screening process for workers and other personnel which include CDC or MDH recommended health questions and consider temperature testing.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> At least one Maryland locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
<td><strong>NOTE:</strong> At least one Maryland locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>No requirement</td>
<td>Required for office spaces, personal care services, laboratories, gyms and fitness centers, lodging establishments, manufacturing, restaurants, retail stores, and &quot;sectors not otherwise addressed.&quot; Facilities must screen workers at each shift by ensuring that workers are not experiencing any of the specified symptoms and have not had close contact with an individual diagnosed with COVID-19.</td>
</tr>
<tr>
<td>Michigan</td>
<td>Required for food selling establishment and pharmacy employees who have indicated that they have had close contact with a person with COVID-19 during the previous 14 days. Employers should measure the</td>
<td>Required for businesses or operations whose employees are required to leave home to work. Conduct a daily entry self-screening protocol for all employees or contractors entering the workplace, including, at a</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td>employee’s temperature and assess symptoms each day before they start work.</td>
<td>minimum, a questionnaire covering symptoms and suspected or confirmed exposure to people with possible COVID-19.</td>
</tr>
<tr>
<td></td>
<td>Ideally, temperature checks should happen before the individual enters the facility.</td>
<td>Required for manufacturing facilities and meat and poultry processing facilities. The employee screening protocol must include temperature screening.</td>
</tr>
<tr>
<td></td>
<td>Required for manufacturing facilities and meat and poultry processing facilities. The employee screening protocol must include temperature screening.</td>
<td>Required for food selling establishments and pharmacies. Such employers must ask employees symptom and contact screening questions as they report for work.</td>
</tr>
<tr>
<td></td>
<td>Required for casinos. The employee screening protocol must include temperature screening.</td>
<td>Required for construction businesses. Conduct a daily entry screening protocol for workers and visitors entering the worksite, including a questionnaire covering symptoms and exposure to people with possible COVID-19, together with, if possible, a temperature screening.</td>
</tr>
<tr>
<td></td>
<td>Recommended for construction businesses and research laboratories, which must conduct temperature screening “if possible.”</td>
<td>Required for manufacturing facilities and meat and poultry processing facilities, which must conduct a daily entry screening protocol for workers, contractors, suppliers, and any other individuals entering the facility, including a questionnaire covering symptoms and suspected or confirmed exposure to people with possible COVID-19. Manufacturers must also create dedicated entry point(s) at every facility for daily screening and ensure physical barriers are in place to prevent anyone from bypassing the screening.</td>
</tr>
</tbody>
</table>

**NOTE:** Some Michigan localities have provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.
<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Temperature Screening</th>
<th>Other Health Screening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minnesota</td>
<td><strong>Recommended</strong>, Employers may opt to conduct temperature screening if it can be done with proper social distancing, protection, and hygiene protocols.</td>
<td><strong>Required</strong>, Employers must establish health screening protocols for workers at the start of each shift (e.g., health screening survey, taking temperature). A health screening must be conducted for each worker upon arrival and check-in at work using the Minnesota Department of Health <a href="https://www.dhs.state.mn.us/dohs/healthy-workplaces">Visitor and Employee Health Screening Checklist</a>.</td>
</tr>
<tr>
<td>Mississippi</td>
<td><strong>No requirement</strong></td>
<td><strong>Required</strong> for restaurants and bars reopening for dine-in; <strong>required</strong> for personal care services employees; <strong>required</strong> for gym and fitness center employees; <strong>required</strong> for employees of indoor places of amusement. Such employers shall conduct a daily screening of all employees at the beginning of their shifts by asking specified questions regarding symptoms. <strong>Required</strong> for all businesses in Bolivar, Calhoun, Carroll, Claiborne, Coahoma, Covington, De Soto, Forrest, Grenada, Harrison, Hinds, Holmes, Humphreys, Jackson, Jefferson, Jones, Lamar, Lee, LeFlore, Lowndes, Madison, Montgomery, Noxubee, Pinola, Pontotoc, Quitman, Rankin, Sharkey, Simpson, Sunflower, Tallahatchie, Tate, Walthall, Washington, Wayne, Winston, and Yalobusha Counties. Employers shall conduct a daily screening of all employees at the beginning of their shifts by asking specified questions regarding symptoms. Employers in the remaining counties are recommended to follow these requirements.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Missouri</td>
<td>No requirement.</td>
<td>No requirement.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Some Missouri localities have provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
<td><strong>NOTE:</strong> Some Missouri localities have provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Montana</td>
<td>No requirement</td>
<td>Required. Employers must conduct health assessments on employees at the beginning of each shift. Personal care services businesses must also screen customers prior to appointments for symptoms.</td>
</tr>
<tr>
<td>Nebraska</td>
<td><strong>Recommended</strong> for restaurants reopening for dine-in. Complete employee pre-screening (e.g., take temperature and assess for any symptoms consistent with COVID-19) prior to starting work.</td>
<td><strong>Recommended</strong> for restaurants reopening for dine-in. Complete employee pre-screening (e.g., take temperature and assess for any symptoms consistent with COVID-19) prior to starting work. <strong>Recommended</strong> for meat processing facilities. All employees and essential visitors/contractors should be screened daily for symptoms.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Nevada</td>
<td>No requirement</td>
<td>Required. The following employers must perform a daily symptom assessment, including monitoring for fever, cough, and trouble breathing: agriculture, appliance and furniture showrooms, auto dealerships, banks and financial services, personal care services, restaurants and food and drink establishments, general office operations, retail and consumer services, and transportation, couriers, and warehousing. Recommended for all employers: have employees perform self-assessments for COVID-19-like symptoms each day. Recommended for grocery employers. Employers should monitor employees for signs of illness and require sick workers to stay home.</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>Required. Essential businesses and organizations and those that are reopening all or a portion of their operations must document the temperature of all employees daily before their shift. Employers should take the temperatures of their employees on-site with a non-touch thermometer each day upon the employees arrival at work. If this is not possible, temperatures can be taken before arriving as long as it can sufficiently be authenticated by the employee. Normal temperature should not exceed 100.0F.</td>
<td>Required. Essential businesses and organizations and those that are reopening all or a portion of their operations must develop a process for screening all employees reporting for work for COVID-19 related symptoms by asking the questions listed in the order. The person responsible for screening should wear a cloth face covering.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>New Jersey</strong></td>
<td><strong>Required</strong> for agriculture employers. Employer is to screen workers for symptoms, including temperature and symptom checks prior to work shifts. <strong>Required</strong> for restaurants and other food and beverage establishments. Employers must conduct daily health checks (e.g., temperature screening and/or symptom checking) of employees safely and respectfully, and in accordance with any applicable privacy laws and regulations.</td>
<td><strong>Required</strong> for agriculture employers. Employer is to screen workers for symptoms, including temperature and symptom checks prior to work shifts. <strong>Required</strong> for restaurants and other food and beverage establishments. Employers must conduct daily health checks (e.g., temperature screening and/or symptom checking) of employees safely and respectfully, and in accordance with any applicable privacy laws and regulations.</td>
</tr>
<tr>
<td><strong>New Mexico</strong></td>
<td><strong>Recommended</strong> as a best practice for retail employers: screen employees and customers with a no-contact thermometer and do not permit entry to those with a temperature greater than 100.4F.</td>
<td><strong>Required</strong>. All employers must screen employees for symptoms before they enter the workplace each day, verbally or with a written or text/app-based questionnaire.</td>
</tr>
<tr>
<td><strong>New York</strong></td>
<td>Recommended generally as part of an employer’s mandatory health screening assessment. Commercial building owners, retail store owners and those authorized on their behalf to manage public places within their buildings and businesses shall have the discretion to require individuals to undergo temperature checks prior to being allowed admittance, as well as the discretion to deny admittance to (i) any individual who refuses to undergo such a temperature check and (ii) any individual whose temperature is above that proscribed by New York State Department of Health Guidelines.</td>
<td>Required. Reopening businesses must adopt the NY Forward Safety Plan, which includes implementing a mandatory health screening assessment (e.g., questionnaire, temperature check) before employees begin work each day and for essential visitors. Assessment responses must be reviewed every day and the review must be documented.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>North Carolina</td>
<td>No requirement.</td>
<td>Required. Businesses open to the public must conduct daily symptom screening of workers, using a standard interview questionnaire of symptoms, before workers enter the workplace.</td>
</tr>
<tr>
<td></td>
<td>NOTE: At least one North Carolina locality has provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
<td>NOTE: At least one North Carolina locality has provisions concerning employee health screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>North Dakota</td>
<td>Recommended. Employers may check employees’ temperatures when they arrive to work.</td>
<td>Recommended. If an employee calls in sick, an employer may ask the employee if they are experiencing symptoms related to COVID-19.</td>
</tr>
<tr>
<td>Ohio</td>
<td>No requirement</td>
<td>Required. Employees must conduct daily health self-assessments and must not report to work if symptomatic.</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>No requirement.</td>
<td>No requirement</td>
</tr>
<tr>
<td></td>
<td>NOTE: Some Oklahoma localities have provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
<td></td>
</tr>
<tr>
<td>Oregon</td>
<td>Recommended. Employers should consider regular health checks (e.g., temperature and respiratory symptom screening) or symptom self-report of employees, if job-related and consistent with business necessity.</td>
<td>Recommended. Employers should consider regular health checks (e.g., temperature and respiratory symptom screening) or symptom self-report of employees, if job-related and consistent with business necessity.</td>
</tr>
<tr>
<td></td>
<td>Personal care services employers should consider temperature checks for clients</td>
<td>Personal care services employers must contact clients prior to appointments to screen them for symptoms.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td><strong>Recommended</strong> generally, required for confirmed exposure. Employers may take employees’ temperatures before they begin work and send employees home if they have a fever of 100.4F or above. If the business has been exposed to a person who is a probable or confirmed case of COVID19, employers shall implement the above temperature screening protocol. <strong>NOTE:</strong> At least one Pennsylvania locality has provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
<td><strong>Required</strong>, All businesses conducting in-person operations must screen workers for symptoms before they enter the business.</td>
</tr>
<tr>
<td>Puerto Rico</td>
<td>No requirement</td>
<td><strong>Required</strong>, Employers must implement a protocol to monitor and screen personnel prior to entering the workplace, along with the procedures to follow in case they detect an employee with symptoms.</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>No requirement</td>
<td><strong>Required</strong>, Businesses must implement and ensure compliance with screening all individuals entering the establishment at any time for any reason including, at minimum: (1) visual assessment, self-screening, or a written questionnaire, or a combination of any of these screening methods; and (2) at all entrances to an establishment, notice that all individuals entering must be screened or self-screened, and to not enter if they are COVID-19 positive, have COVID-19 symptoms, or have had close contact with a COVID-19-positive individual.</td>
</tr>
<tr>
<td>South Carolina</td>
<td><strong>Recommended</strong> for restaurant employees.</td>
<td><strong>Recommended</strong> for restaurant employees.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>South Dakota</td>
<td>No requirement</td>
<td>Recommended. Employers can ask employees screening questions when they report to work and keep a daily screening log.</td>
</tr>
<tr>
<td>Tennessee</td>
<td>Recommended, “Best practice:” employers to take temperatures on site with a no-touch thermometer each day upon arrival at work. “Minimum:” Temperatures can be taken before arriving. Normal temperature should not exceed 100.4F.</td>
<td>Recommended. Screen employees with questions about symptoms. NOTE: Some Tennessee localities have provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Texas</td>
<td>Recommended as a minimum standard health protocol for businesses that are reopening. All employees should be screened before coming into the business for specified symptoms consistent with COVID-19, including feeling feverish or a measured temperature of 100.0F or greater.</td>
<td>Recommended as a minimum standard health protocol for businesses that are reopening. All employees should be screened before coming into the business for specified symptoms consistent with COVID-19 or known close contact with a person who is lab-confirmed to have COVID-19. Any employee who meets any of these criteria should be sent home. NOTE: Some Texas localities have provisions concerning employee temperature screenings. Please check with your Littler attorney for additional information about your particular jurisdiction.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Utah</td>
<td>Required for <strong>gyms/fitness centers</strong>: Employees must go through symptom checking before every shift, including temperature.</td>
<td>Required for <strong>gyms/fitness centers</strong> and <strong>personal care services</strong>: Symptom checking of all staff at the beginning of each shift, with a log that can be made available for inspection by health department. Recommended for <strong>all employers</strong>: employees who are, or work with, high-risk populations, should undergo daily screening/symptom monitoring.</td>
</tr>
<tr>
<td>Vermont</td>
<td><strong>Required</strong>. To the extent feasible, prior to the commencement of each work shift, prescreening or survey shall be required to verify each employee has no symptoms of respiratory illness, including temperature checks.</td>
<td><strong>Required</strong>. To the extent feasible, prior to the commencement of each work shift, prescreening or survey shall be required to verify each employee has no symptoms of respiratory illness, including temperature checks.</td>
</tr>
<tr>
<td>Virginia</td>
<td><strong>Recommended</strong> generally. Employees should also self-monitor their symptoms by self-taking of temperature to check for fever before reporting to work. For employers with established occupational health programs, employers can consider measuring temperature and assessing symptoms of employees prior to starting work/before each shift.</td>
<td><strong>Recommended</strong> for employers with hazards or job tasks classified as “medium,” “high,” or “very high.” Prior to the commencement of each work shift, prescreening or surveying shall be required to verify each covered employee does not have signs or symptoms of COVID-19. <strong>Recommended</strong> generally. Prior to a shift and on days employees are scheduled to work, employers should screen employees prior to starting work. Employees should also self-monitor their symptoms by self-taking of temperature to check for fever and utilizing the questions provided in the VDH Interim Guidance for COVID-19 Daily Screening of Employees before reporting to work. For employers with established occupational health programs, employers can consider measuring temperature and assessing symptoms of employees prior to starting work/before each shift.</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Washington</strong></td>
<td><strong>Required</strong> for reopening nonessential retail establishments. Employers must ask employees to take their temperatures at home prior to arriving at work or take their temperatures when they arrive. Thermometers used shall be 'no touch' or 'no contact' to the greatest extent possible. Any worker with a temperature of 100.4°F or higher is considered to have a fever and must be sent home. <strong>Required</strong> on low-risk construction sites. Employers must take each worker's temperature at the beginning of their shift. Thermometers used shall be 'no touch' or 'no contact' to the greatest extent possible. If a 'no touch' or 'no contact' thermometer is not available, the thermometer must be properly sanitized between each use. Any worker with a temperature of 100.4°F or higher is considered to have a fever and must be sent home.</td>
<td><strong>Recommended</strong>. All employers are advised to screen everyone who enters their facility, including all employees before the start of each work shift and all visitors. The guidance lists suggested screening questions. <strong>Required</strong> for restaurants. Employers must screen employees for signs and symptoms of COVID-19 at the start of shift. <strong>Required</strong> on low-risk construction sites. Employers must screen all workers at the beginning of their shift by asking them if they have any of the specified symptoms. <strong>Required</strong> for reopening nonessential retail establishments. Employees must be screened for signs and symptoms of COVID-19 at the start of every shift. <strong>Required</strong> for landscaping employers. Employees must be screened for signs and symptoms of COVID-19 at the start of every shift.</td>
</tr>
<tr>
<td><strong>West Virginia</strong></td>
<td>Recommended for lodging establishments and restaurants. Employees are encouraged to take their temperature prior to leaving for work or upon arrival. If their temperature measures over 100°F, the employee should notify management and not begin work.</td>
<td>Required for certain employers. Restaurant and bar employers and lodging establishments and retail establishments must monitor their employees daily by asking screening questions about common symptoms of COVID-19. Small businesses are recommended to screen employees for COVID-19 symptoms daily using a series of questions.</td>
</tr>
<tr>
<td><strong>Wisconsin</strong></td>
<td>No requirement</td>
<td>No requirement</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Temperature Screening</td>
<td>Other Health Screening</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Wyoming</td>
<td>No requirement</td>
<td>Required. Restaurant/bar employees, movie theater and live performance venue employees must be screened for symptoms of illness before each shift. Required. Gym employees must be screened for symptoms of illness before each shift. Required. Personal care services employees must be screened for symptoms of illness before each shift. Generally recommended for other employers.</td>
</tr>
</tbody>
</table>

Information contained in this publication is intended for informational purposes only and does not constitute legal advice or opinion, nor is it a substitute for the professional judgment of an attorney.
What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws

Technical Assistance Questions and Answers - Updated on Sep. 8, 2020

INTRODUCTION

- All EEOC materials related to COVID-19 are collected at [www.eeoc.gov/coronavirus](http://www.eeoc.gov/coronavirus).
- The EEOC enforces workplace anti-discrimination laws, including the Americans with Disabilities Act (ADA) and the Rehabilitation Act (which include the requirement for reasonable accommodation and non-discrimination based on disability, and rules about employer medical examinations and inquiries), Title VII of the Civil Rights Act (which prohibits discrimination based on race, color, national origin, religion, and sex, including pregnancy), the Age Discrimination in Employment Act (which prohibits discrimination based on age, 40 or older), and the Genetic Information Nondiscrimination Act. Note: Other federal laws, as well as state or local laws, may provide employees with additional protections.
- Title I of the ADA applies to private employers with 15 or more employees. It also applies to state and local government employers, employment agencies, and labor unions. All nondiscrimination standards under Title I of the ADA also apply to federal agencies under Section 501 of the Rehabilitation Act. Basic background information about the ADA and the Rehabilitation Act is available on EEOC’s [disability page](http://www.eeoc.gov/laws/types/disability.cfm).
- The EEO laws, including the ADA and Rehabilitation Act, continue to apply during the time of the COVID-19 pandemic, but they do not interfere with or prevent employers from following the [guidelines and suggestions made by the CDC or state/local public health authorities](https://www.cdc.gov/). Employers should remember that guidance from public health authorities is likely to change as the COVID-19 pandemic evolves. Therefore, employers should continue to follow the most current information on maintaining workplace safety. Many common workplace inquiries about the COVID-19 pandemic are addressed in the CDC publication “[General Business Frequently Asked Questions](https://www.cdc.gov/coronavirus/2019-ncov/guidance/business-faqs.html).”
- The EEOC has provided guidance (a publication entitled [Pandemic Preparedness in the Workplace and the Americans With Disabilities Act](https://www.eeoc.gov/file/11415/download) ([PDF version]), “Pandemic Preparedness”), consistent with these workplace protections and rules, that can help employers implement strategies to navigate the impact of COVID-19 in the workplace. This pandemic publication, which was written during the prior H1N1 outbreak, is still relevant today and identifies established ADA and Rehabilitation Act principles to answer questions frequently asked about the workplace during a pandemic. It has been updated as of March 19, 2020 to address examples and information regarding COVID-19; the new 2020 information appears in bold and is marked with an asterisk.
On March 27, 2020 the EEOC provided a webinar ("3/27/20 Webinar") which was recorded and transcribed and is available at www.eeoc.gov/coronavirus. The World Health Organization (WHO) has declared COVID-19 to be an international pandemic. The EEOC pandemic publication includes a separate section that answers common employer questions about what to do after a pandemic has been declared. Applying these principles to the COVID-19 pandemic, the following may be useful:

**A. Disability-Related Inquiries and Medical Exams**

The ADA has restrictions on when and how much medical information an employer may obtain from any applicant or employee. Prior to making a conditional job offer to an applicant, disability-related inquiries and medical exams are generally prohibited. They are permitted between the time of the offer and when the applicant begins work, provided they are required for everyone in the same job category. Once an employee begins work, any disability-related inquiries or medical exams must be job related and consistent with business necessity.

**A.1. How much information may an employer request from an employee who calls in sick, in order to protect the rest of its workforce during the COVID-19 pandemic?** (3/17/20)

During a pandemic, ADA-covered employers may ask such employees if they are experiencing symptoms of the pandemic virus. For COVID-19, these include symptoms such as fever, chills, cough, shortness of breath, or sore throat. Employers must maintain all information about employee illness as a confidential medical record in compliance with the ADA.

**A.2. When screening employees entering the workplace during this time, may an employer only ask employees about the COVID-19 symptoms EEOC has identified as examples, or may it ask about any symptoms identified by public health authorities as associated with COVID-19?** (4/9/20)

As public health authorities and doctors learn more about COVID-19, they may expand the list of associated symptoms. Employers should rely on the CDC, other public health authorities, and reputable medical sources for guidance on emerging symptoms associated with the disease. These sources may guide employers when choosing questions to ask employees to determine whether they would pose a direct threat to health in the workplace. For example, additional symptoms beyond fever or cough may include new loss of smell or taste as well as gastrointestinal problems, such as nausea, diarrhea, and vomiting.

**A.3. When may an ADA-covered employer take the body temperature of employees during the COVID-19 pandemic?** (3/17/20)

Generally, measuring an employee’s body temperature is a medical examination. Because the CDC and state/local health authorities have acknowledged community spread of COVID-19 and issued attendant precautions, employers may measure employees' body temperature. However, employers should be aware that some people with COVID-19 do not have a fever.

**A.4. Does the ADA allow employers to require employees to stay home if they have symptoms of the COVID-19?** (3/17/20)

Yes. The CDC states that employees who become ill with symptoms of COVID-19 should leave the workplace. The ADA does not interfere with employers following this advice.
**A.5. When employees return to work, does the ADA allow employers to require a doctor’s note certifying fitness for duty?** (3/17/20)

Yes. Such inquiries are permitted under the ADA either because they would not be disability-related or, if the pandemic were truly severe, they would be justified under the ADA standards for disability-related inquiries of employees. As a practical matter, however, doctors and other health care professionals may be too busy during and immediately after a pandemic outbreak to provide fitness-for-duty documentation. Therefore, new approaches may be necessary, such as reliance on local clinics to provide a form, a stamp, or an e-mail to certify that an individual does not have the pandemic virus.

**A.6. May an employer administer a COVID-19 test (a test to detect the presence of the COVID-19 virus) when evaluating an employee’s initial or continued presence in the workplace?** (4/23/20; updated 9/8/20 to address stakeholder questions about updates to CDC guidance)

The ADA requires that any mandatory medical test of employees be “job related and consistent with business necessity.” Applying this standard to the current circumstances of the COVID-19 pandemic, employers may take screening 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 initially permitting them to enter the workplace and/or periodically to determine if their presence in the workplace poses a direct threat to others. The ADA does not interfere with employers following recommendations by the CDC or other public health authorities regarding whether, when, and for whom testing or other screening is appropriate. Testing administered by employers consistent with current CDC guidance will meet the ADA’s “business necessity” standard.

Consistent with the ADA standard, employers should ensure that the tests are considered accurate and reliable. For example, employers may review information from the U.S. Food and Drug Administration about what may or may not be considered safe and accurate testing, as well as guidance from CDC or other public health authorities. Because the CDC and FDA may revise their recommendations based on new information, it may be helpful to check these agency websites for updates. Employers may wish to consider the incidence of false-positives or false-negatives associated with a particular test. Note that a positive test result reveals that an individual most likely has a current infection and may be able to transmit the virus to others. A negative test result means that the individual did not have detectable COVID-19 at the time of testing.

A negative test does not mean the employee will not acquire the virus later. Based on guidance from medical and public health authorities, employers should still require—to the greatest extent possible—that employees observe infection control practices (such as social distancing, regular handwashing, and other measures) in the workplace to prevent transmission of COVID-19.

*Note: Question A.6 and A.8 address screening of employees generally. See Question A.9 regarding decisions to screen individual employees.*

**A.7. CDC said in its Interim Guidelines that antibody test results “should not be used to make decisions about returning persons to the workplace.” In light of this CDC guidance, under the ADA may an employer require antibody testing before permitting employees to re-enter the workplace?** (6/17/20)

No. An antibody test constitutes a medical examination under the ADA. In light of CDC’s Interim Guidelines that antibody test results “should not be used to make decisions about returning persons to the workplace,” an antibody test at this time does not meet the ADA’s “job related and consistent with business necessity” standard for medical examinations or inquiries for current employees. Therefore, requiring antibody testing before allowing employees to re-enter the workplace is not allowed under the ADA.
note that an antibody test is different from a test to determine if someone has an active case of COVID-19 (i.e., a viral test). The EEOC has already stated that COVID-19 viral tests are permissible under the ADA.

The EEOC will continue to closely monitor CDC’s recommendations, and could update this discussion in response to changes in CDC’s recommendations.

A.8. May employers ask all employees physically entering the workplace if they have been diagnosed with or tested for COVID-19? (9/8/20; adapted from 3/27/20 Webinar Question 1)

Yes. Employers may ask all employees who will be physically entering the workplace if they have COVID-19 or symptoms associated with COVID-19, and ask if they have been tested for COVID-19. Symptoms associated with COVID-19 include, for example, fever, chills, cough, and shortness of breath. The CDC has identified a current list of symptoms.

An employer may exclude those with COVID-19, or symptoms associated with COVID-19, from the workplace because, as EEOC has stated, their presence would pose a direct threat to the health or safety of others. However, for those employees who are teleworking and are not physically interacting with coworkers or others (for example, customers), the employer would generally not be permitted to ask these questions.

A.9. May a manager ask only one employee—as opposed to asking all employees—questions designed to determine if she has COVID-19, or require that this employee alone have her temperature taken or undergo other screening or testing? (9/8/20; adapted from 3/27/20 Webinar Question 3)

If an employer wishes to ask only a particular employee to answer such questions, or to have her temperature taken or undergo other screening or testing, the ADA requires the employer to have a reasonable belief based on objective evidence that this person might have the disease. So, it is important for the employer to consider why it wishes to take these actions regarding this particular employee, such as a display of COVID-19 symptoms. In addition, the ADA does not interfere with employers following recommendations by the CDC or other public health authorities regarding whether, when, and for whom testing or other screening is appropriate.

A.10. May an employer ask an employee who is physically coming into the workplace whether they have family members who have COVID-19 or symptoms associated with COVID-19? (9/8/20; adapted from 3/27/20 Webinar Question 4)

No. The Genetic Information Nondiscrimination Act (GINA) prohibits employers from asking employees medical questions about family members. GINA, however, does not prohibit an employer from asking employees whether they have had contact with anyone diagnosed with COVID-19 or who may have symptoms associated with the disease. Moreover, from a public health perspective, only asking an employee about his contact with family members would unnecessarily limit the information obtained about an employee’s potential exposure to COVID-19.

A.11. What may an employer do under the ADA if an employee refuses to permit the employer to take his temperature or refuses to answer questions about whether he has COVID-19, has symptoms associated with COVID-19, or has been tested for COVID-19? (9/8/20; adapted from 3/27/20 Webinar Question 2)

Under the circumstances existing currently, the ADA allows an employer to bar an employee from physical presence in the workplace if he refuses to have his temperature taken or refuses to answer questions about whether he has COVID-19, has symptoms associated with COVID-19, or has been tested for COVID-19. To gain
the cooperation of employees, however, employers may wish to ask the reasons for the employee's refusal. The employer may be able to provide information or reassurance that they are taking these steps to ensure the safety of everyone in the workplace, and that these steps are consistent with health screening recommendations from CDC. Sometimes, employees are reluctant to provide medical information because they fear an employer may widely spread such personal medical information throughout the workplace. The ADA prohibits such broad disclosures. Alternatively, if an employee requests reasonable accommodation with respect to screening, the usual accommodation process should be followed; this is discussed in Question G.7.

A.12. During the COVID-19 pandemic, may an employer request information from employees who work on-site, whether regularly or occasionally, who report feeling ill or who call in sick? (9/8/20; adapted from Pandemic Preparedness Question 6)

Due to the COVID-19 pandemic, at this time employers may ask employees who work on-site, whether regularly or occasionally, and report feeling ill or who call in sick, questions about their symptoms as part of workplace screening for COVID-19.

A.13. May an employer ask an employee why he or she has been absent from work? (9/8/20; adapted from Pandemic Preparedness Question 15)

Yes. Asking why an individual did not report to work is not a disability-related inquiry. An employer is always entitled to know why an employee has not reported for work.

A.14. When an employee returns from travel during a pandemic, must an employer wait until the employee develops COVID-19 symptoms to ask questions about where the person has traveled? (9/8/20; adapted from Pandemic Preparedness Question 8)

No. Questions about where a person traveled would not be disability-related inquiries. If the CDC or state or local public health officials recommend that people who visit specified locations remain at home for a certain period of time, an employer may ask whether employees are returning from these locations, even if the travel was personal.

B. Confidentiality of Medical Information

With limited exceptions, the ADA requires employers to keep confidential any medical information they learn about any applicant or employee. Medical information includes not only a diagnosis or treatments, but also the fact that an individual has requested or is receiving a reasonable accommodation.

B.1. May an employer store in existing medical files information it obtains related to COVID-19, including the results of taking an employee's temperature or the employee's self-identification as having this disease, or must the employer create a new medical file system solely for this information? (4/9/20)

The ADA requires that all medical information about a particular employee be stored separately from the employee's personnel file, thus limiting access to this confidential information. An employer may store all medical information related to COVID-19 in existing medical files. This includes an employee's statement that he has the disease or suspects he has the disease, or the employer's notes or other documentation from questioning an employee about symptoms.
B.2. If an employer requires all employees to have a daily temperature check before entering the workplace, may the employer maintain a log of the results? (4/9/20)

Yes. The employer needs to maintain the confidentiality of this information.

B.3. May an employer disclose the name of an employee to a public health agency when it learns that the employee has COVID-19? (4/9/20)

Yes.

B.4. May a temporary staffing agency or a contractor that places an employee in an employer’s workplace notify the employer if it learns the employee has COVID-19? (4/9/20)

Yes. The staffing agency or contractor may notify the employer and disclose the name of the employee, because the employer may need to determine if this employee had contact with anyone in the workplace.

B.5. Suppose a manager learns that an employee has COVID-19, or has symptoms associated with the disease. The manager knows she must report it but is worried about violating ADA confidentiality. What should she do? (9/8/20; adapted from 3/27/20 Webinar Question 5)

The ADA requires that an employer keep all medical information about employees confidential, even if that information is not about a disability. Clearly, the information that an employee has symptoms of, or a diagnosis of, COVID-19, is medical information. But the fact that this is medical information does not prevent the manager from reporting to appropriate employer officials so that they can take actions consistent with guidance from the CDC and other public health authorities.

The question is really what information to report: is it the fact that an employee—unnamed—has symptoms of COVID-19 or a diagnosis, or is it the identity of that employee? Who in the organization needs to know the identity of the employee will depend on each workplace and why a specific official needs this information. Employers should make every effort to limit the number of people who get to know the name of the employee.

The ADA does not interfere with a designated representative of the employer interviewing the employee to get a list of people with whom the employee possibly had contact through the workplace, so that the employer can then take action to notify those who may have come into contact with the employee, without revealing the employee’s identity. For example, using a generic descriptor, such as telling employees that “someone at this location” or “someone on the fourth floor” has COVID-19, provides notice and does not violate the ADA’s prohibition of disclosure of confidential medical information. For small employers, coworkers might be able to figure out who the employee is, but employers in that situation are still prohibited from confirming or revealing the employee’s identity. Also, all employer officials who are designated as needing to know the identity of an employee should be specifically instructed that they must maintain the confidentiality of this information. Employers may want to plan in advance what supervisors and managers should do if this situation arises and determine who will be responsible for receiving information and taking next steps.

B.6. An employee who must report to the workplace knows that a coworker who reports to the same workplace has symptoms associated with COVID-19. Does ADA confidentiality prevent the first employee from disclosing the coworker’s symptoms to a supervisor? (9/8/20; adapted from 3/27/20 Webinar Question 6)

No. ADA confidentiality does not prevent this employee from communicating to his supervisor about a coworker’s symptoms. In other words, it is not an ADA confidentiality violation for this employee to inform his
supervisor about a coworker's symptoms. After learning about this situation, the supervisor should contact appropriate management officials to report this information and discuss next steps.

B.7. An employer knows that an employee is teleworking because the person has COVID-19 or symptoms associated with the disease, and that he is in self-quarantine. May the employer tell staff that this particular employee is teleworking without saying why? (9/8/20; adapted from 3/27/20 Webinar Question 7)

Yes. If staff need to know how to contact the employee, and that the employee is working even if not present in the workplace, then disclosure that the employee is teleworking without saying why is permissible. Also, if the employee was on leave rather than teleworking because he has COVID-19 or symptoms associated with the disease, or any other medical condition, then an employer cannot disclose the reason for the leave, just the fact that the individual is on leave.

B.8. Many employees, including managers and supervisors, are now teleworking as a result of COVID-19. How are they supposed to keep medical information of employees confidential while working remotely? (9/8/20; adapted from 3/27/20 Webinar Question 9)

The ADA requirement that medical information be kept confidential includes a requirement that it be stored separately from regular personnel files. If a manager or supervisor receives medical information involving COVID-19, or any other medical information, while teleworking, and is able to follow an employer’s existing confidentiality protocols while working remotely, the supervisor has to do so. But to the extent that is not feasible, the supervisor still must safeguard this information to the greatest extent possible until the supervisor can properly store it. This means that paper notepads, laptops, or other devices should not be left where others can access the protected information.

Similarly, documentation must not be stored electronically where others would have access. A manager may even wish to use initials or another code to further ensure confidentiality of the name of an employee.

C. Hiring and Onboarding

Under the ADA, prior to making a conditional offer to an applicant, disability-related inquiries and medical exams are generally prohibited. They are permitted between the time of the offer and when the applicant begins work, provided they are required for everyone in the same job category.

C.1. If an employer is hiring, may it screen applicants for symptoms of COVID-19? (3/18/20)

Yes. An employer may screen job applicants for symptoms of COVID-19 after making a conditional offer, as long as it does so for all entering employees in the same type of job. This ADA rule applies whether or not the applicant has a disability.

C.2. May an employer take an applicant's temperature as part of a post-offer, pre-employment medical exam? (3/18/20)

Yes. Any medical exams are permitted after an employer has made a conditional offer of employment. However, employers should be aware that some people with COVID-19 do not have a fever.

C.3. May an employer delay the start date of an applicant who has COVID-19 or symptoms associated with it? (3/18/20)
Yes. According to current CDC guidance, an individual who has COVID-19 or symptoms associated with it should not be in the workplace.

C.4. **May an employer withdraw a job offer when it needs the applicant to start immediately but the individual has COVID-19 or symptoms of it?** (3/18/20)

Based on current CDC guidance, this individual cannot safely enter the workplace, and therefore the employer may withdraw the job offer.

C.5. **May an employer postpone the start date or withdraw a job offer because the individual is 65 years old or pregnant, both of which place them at higher risk from COVID-19?** (4/9/20)

No. The fact that the CDC has identified those who are 65 or older, or pregnant women, as being at greater risk does not justify unilaterally postponing the start date or withdrawing a job offer. However, an employer may choose to allow telework or to discuss with these individuals if they would like to postpone the start date.

**D. Reasonable Accommodation**

*Under the ADA, reasonable accommodations are adjustments or modifications provided by an employer to enable people with disabilities to enjoy equal employment opportunities. If a reasonable accommodation is needed and requested by an individual with a disability to apply for a job, perform a job, or enjoy benefits and privileges of employment, the employer must provide it unless it would pose an undue hardship, meaning significant difficulty or expense. An employer has the discretion to choose among effective accommodations. Where a requested accommodation would result in undue hardship, the employer must offer an alternative accommodation if one is available absent undue hardship. In discussing accommodation requests, employers and employees may find it helpful to consult the Job Accommodation Network (JAN) website for types of accommodations, [www.askjan.org](http://www.askjan.org). JAN's materials specific to COVID-19 are at [https://askjan.org/topics/COVID-19.cfm](https://askjan.org/topics/COVID-19.cfm).*

D.1. **If a job may only be performed at the workplace, are there reasonable accommodations for individuals with disabilities, absent undue hardship, that could offer protection to an employee who, due to a preexisting disability, is at higher risk from COVID-19?** (4/9/20)

There may be reasonable accommodations that *could offer protection to an individual whose disability puts him at greater risk from COVID-19* and who therefore requests such actions to eliminate possible exposure. Even with the constraints imposed by a pandemic, some accommodations may meet an employee's needs on a temporary basis without causing undue hardship on the employer.

Low-cost solutions achieved with materials already on hand or easily obtained may be effective. If not already implemented for all employees, accommodations for those who request reduced contact with others due to a disability may include changes to the work environment such as designating one-way aisles; using plexiglass, tables, or other barriers to ensure minimum distances between customers and coworkers whenever feasible per [CDC guidance](https://www.cdc.gov/), or other accommodations that reduce chances of exposure.

Flexibility by employers and employees is important in determining if some accommodation is possible in the circumstances. Temporary job restructuring of marginal job duties, temporary transfers to a different position, or modifying a work schedule or shift assignment may also permit an individual with a disability to perform safely the essential functions of the job while reducing exposure to others in the workplace or while commuting.
D.2. If an employee has a preexisting mental illness or disorder that has been exacerbated by the COVID-19 pandemic, may he now be entitled to a reasonable accommodation (absent undue hardship)? (4/9/20)

Although many people feel significant stress due to the COVID-19 pandemic, employees with certain preexisting mental health conditions, for example, anxiety disorder, obsessive-compulsive disorder, or post-traumatic stress disorder, may have more difficulty handling the disruption to daily life that has accompanied the COVID-19 pandemic.

As with any accommodation request, employers may: ask questions to determine whether the condition is a disability; discuss with the employee how the requested accommodation would assist him and enable him to keep working; explore alternative accommodations that may effectively meet his needs; and request medical documentation if needed.

D.3. In a workplace where all employees are required to telework during this time, should an employer postpone discussing a request from an employee with a disability for an accommodation that will not be needed until he returns to the workplace when mandatory telework ends? (4/9/20)

Not necessarily. An employer may give higher priority to discussing requests for reasonable accommodations that are needed while teleworking, but the employer may begin discussing this request now. The employer may be able to acquire all the information it needs to make a decision. If a reasonable accommodation is granted, the employer also may be able to make some arrangements for the accommodation in advance.

D.4. What if an employee was already receiving a reasonable accommodation prior to the COVID-19 pandemic and now requests an additional or altered accommodation? (4/9/20)

An employee who was already receiving a reasonable accommodation prior to the COVID-19 pandemic may be entitled to an additional or altered accommodation, absent undue hardship. For example, an employee who is teleworking because of the pandemic may need a different type of accommodation than what he uses in the workplace. The employer may discuss with the employee whether the same or a different disability is the basis for this new request and why an additional or altered accommodation is needed.

D.5. During the pandemic, if an employee requests an accommodation for a medical condition either at home or in the workplace, may an employer still request information to determine if the condition is a disability? (4/17/20)

Yes, if it is not obvious or already known, an employer may ask questions or request medical documentation to determine whether the employee has a "disability" as defined by the ADA (a physical or mental impairment that substantially limits a major life activity, or a history of a substantially limiting impairment).

D.6. During the pandemic, may an employer still engage in the interactive process and request information from an employee about why an accommodation is needed? (4/17/20)

Yes, if it is not obvious or already known, an employer may ask questions or request medical documentation to determine whether the employee's disability necessitates an accommodation, either the one he requested or any other. Possible questions for the employee may include: (1) how the disability creates a limitation, (2) how the requested accommodation will effectively address the limitation, (3) whether another form of accommodation could effectively address the issue, and (4) how a proposed accommodation will enable the employee to continue performing the "essential functions" of his position (that is, the fundamental job duties).
D.7. If there is some urgency to providing an accommodation, or the employer has limited time available to discuss the request during the pandemic, may an employer provide a temporary accommodation? (4/17/20)

Yes. Given the pandemic, some employers may choose to forgo or shorten the exchange of information between an employer and employee known as the "interactive process" (discussed in D.5 and D.6., above) and grant the request. In addition, when government restrictions change, or are partially or fully lifted, the need for accommodations may also change. This may result in more requests for short-term accommodations. Employers may wish to adapt the interactive process—and devise end dates for the accommodation—to suit changing circumstances based on public health directives.

Whatever the reason for shortening or adapting the interactive process, an employer may also choose to place an end date on the accommodation (for example, either a specific date such as May 30, or when the employee returns to the workplace part- or full-time due to changes in government restrictions limiting the number of people who may congregate). Employers may also opt to provide a requested accommodation on an interim or trial basis, with an end date, while awaiting receipt of medical documentation. Choosing one of these alternatives may be particularly helpful where the requested accommodation would provide protection that an employee may need because of a pre-existing disability that puts her at greater risk during this pandemic. This could also apply to employees who have disabilities exacerbated by the pandemic.

Employees may request an extension that an employer must consider, particularly if current government restrictions are extended or new ones adopted.

D.8. May an employer invite employees now to ask for reasonable accommodations they may need in the future when they are permitted to return to the workplace? (4/17/20; updated 9/8/20 to address stakeholder questions)

Yes. Employers may inform the workforce that employees with disabilities may request accommodations in advance that they believe they may need when the workplace re-opens. If advance requests are received, employers may begin the "interactive process" – the discussion between the employer and employee focused on whether the impairment is a disability and the reasons that an accommodation is needed. If an employee chooses not to request accommodation in advance, and instead requests it at a later time, the employer must still consider the request at that time.

D.9. Are the circumstances of the pandemic relevant to whether a requested accommodation can be denied because it poses an undue hardship? (4/17/20)

Yes. An employer does not have to provide a particular reasonable accommodation if it poses an "undue hardship," which means "significant difficulty or expense." As described in the two questions that follow, in some instances, an accommodation that would not have posed an undue hardship prior to the pandemic may pose one now.

D.10. What types of undue hardship considerations may be relevant to determine if a requested accommodation poses "significant difficulty" during the COVID-19 pandemic? (4/17/20)

An employer may consider whether current circumstances create "significant difficulty" in acquiring or providing certain accommodations, considering the facts of the particular job and workplace. For example, it may be significantly more difficult in this pandemic to conduct a needs assessment or to acquire certain items, and delivery may be impacted, particularly for employees who may be teleworking. Or, it may be significantly more difficult to provide employees with temporary assignments, to remove marginal functions,
or to readily hire temporary workers for specialized positions. If a particular accommodation poses an undue hardship, employers and employees should work together to determine if there may be an alternative that could be provided that does not pose such problems.

D.11. What types of undue hardship considerations may be relevant to determine if a requested accommodation poses "significant expense" during the COVID-19 pandemic? (4/17/20)

Prior to the COVID-19 pandemic, most accommodations did not pose a significant expense when considered against an employer’s overall budget and resources (always considering the budget/resources of the entire entity and not just its components). But, the sudden loss of some or all of an employer’s income stream because of this pandemic is a relevant consideration. Also relevant is the amount of discretionary funds available at this time—when considering other expenses—and whether there is an expected date that current restrictions on an employer’s operations will be lifted (or new restrictions will be added or substituted). These considerations do not mean that an employer can reject any accommodation that costs money; an employer must weigh the cost of an accommodation against its current budget while taking into account constraints created by this pandemic. For example, even under current circumstances, there may be many no-cost or very low-cost accommodations.

D.12. Do the ADA and the Rehabilitation Act apply to applicants or employees who are classified as “critical infrastructure workers” or “essential critical workers” by the CDC? (4/23/20)

Yes. These CDC designations, or any other designations of certain employees, do not eliminate coverage under the ADA or the Rehabilitation Act, or any other equal employment opportunity law. Therefore, employers receiving requests for reasonable accommodation under the ADA or the Rehabilitation Act from employees falling in these categories of jobs must accept and process the requests as they would for any other employee. Whether the request is granted will depend on whether the worker is an individual with a disability, and whether there is a reasonable accommodation that can be provided absent undue hardship.

D.13. Is an employee entitled to an accommodation under the ADA in order to avoid exposing a family member who is at higher risk of severe illness from COVID-19 due to an underlying medical condition? (6/11/20)

No. Although the ADA prohibits discrimination based on association with an individual with a disability, that protection is limited to disparate treatment or harassment. The ADA does not require that an employer accommodate an employee without a disability based on the disability-related needs of a family member or other person with whom she is associated.

For example, an employee without a disability is not entitled under the ADA to telework as an accommodation in order to protect a family member with a disability from potential COVID-19 exposure.

Of course, an employer is free to provide such flexibilities if it chooses to do so. An employer choosing to offer additional flexibilities beyond what the law requires should be careful not to engage in disparate treatment on a protected EEO basis.

D.14. When an employer requires some or all of its employees to telework because of COVID-19 or government officials require employers to shut down their facilities and have workers telework, is the employer required to provide a teleworking employee with the same reasonable accommodations for disability under the ADA or the Rehabilitation Act that it provides to this individual in the workplace? (9/8/20; adapted from 3/27/20 Webinar Question 20)
If such a request is made, the employer and employee should discuss what the employee needs and why, and whether the same or a different accommodation could suffice in the home setting. For example, an employee may already have certain things in their home to enable them to do their job so that they do not need to have all of the accommodations that are provided in the workplace.

Also, the undue hardship considerations might be different when evaluating a request for accommodation when teleworking rather than working in the workplace. A reasonable accommodation that is feasible and does not pose an undue hardship in the workplace might pose one when considering circumstances, such as the place where it is needed and the reason for telework. For example, the fact that the period of telework may be of a temporary or unknown duration may render certain accommodations either not feasible or an undue hardship. There may also be constraints on the normal availability of items or on the ability of an employer to conduct a necessary assessment.

As a practical matter, and in light of the circumstances that led to the need for telework, employers and employees should both be creative and flexible about what can be done when an employee needs a reasonable accommodation for telework at home. If possible, providing interim accommodations might be appropriate while an employer discusses a request with the employee or is waiting for additional information.

D.15. Assume that an employer grants telework to employees for the purpose of slowing or stopping the spread of COVID-19. When an employer reopens the workplace and recalls employees to the worksite, does the employer automatically have to grant telework as a reasonable accommodation to every employee with a disability who requests to continue this arrangement as an ADA/Rehabilitation Act accommodation? (9/8/20; adapted from 3/27/20 Webinar Question 21)

No. Any time an employee requests a reasonable accommodation, the employer is entitled to understand the disability-related limitation that necessitates an accommodation. If there is no disability-related limitation that requires teleworking, then the employer does not have to provide telework as an accommodation. Or, if there is a disability-related limitation but the employer can effectively address the need with another form of reasonable accommodation at the workplace, then the employer can choose that alternative to telework.

To the extent that an employer is permitting telework to employees because of COVID-19 and is choosing to excuse an employee from performing one or more essential functions, then a request—afer the workplace reopens—to continue telework as a reasonable accommodation does not have to be granted if it requires continuing to excuse the employee from performing an essential function. The ADA never requires an employer to eliminate an essential function as an accommodation for an individual with a disability.

The fact that an employer temporarily excused performance of one or more essential functions when it closed the workplace and enabled employees to telework for the purpose of protecting their safety from COVID-19, or otherwise chose to permit telework, does not mean that the employer permanently changed a job’s essential functions, that telework is always a feasible accommodation, or that it does not pose an undue hardship. These are fact-specific determinations. The employer has no obligation under the ADA to refrain from restoring all of an employee’s essential duties at such time as it chooses to restore the prior work arrangement, and then evaluating any requests for continued or new accommodations under the usual ADA rules.

D.16. Assume that prior to the emergence of the COVID-19 pandemic, an employee with a disability had requested telework as a reasonable accommodation. The employee had shown a disability-related need for this accommodation, but the employer denied it because of concerns that the employee would not be able to perform the essential functions remotely. In the past, the employee therefore continued to
come to the workplace. However, after the COVID-19 crisis has subsided and temporary telework ends, the employee renews her request for telework as a reasonable accommodation. Can the employer again refuse the request? (9/8/20; adapted from 3/27/20 Webinar Question 22)

Assuming all the requirements for such a reasonable accommodation are satisfied, the temporary telework experience could be relevant to considering the renewed request. In this situation, for example, the period of providing telework because of the COVID-19 pandemic could serve as a trial period that showed whether or not this employee with a disability could satisfactorily perform all essential functions while working remotely, and the employer should consider any new requests in light of this information. As with all accommodation requests, the employee and the employer should engage in a flexible, cooperative interactive process going forward if this issue does arise.

D.17. Might the pandemic result in excusable delays during the interactive process? (9/8/20; adapted from 3/27/20 Webinar Question 19)

Yes. The rapid spread of COVID-19 has disrupted normal work routines and may have resulted in unexpected or increased requests for reasonable accommodation. Although employers and employees should address these requests as soon as possible, the extraordinary circumstances of the COVID-19 pandemic may result in delay in discussing requests and in providing accommodation where warranted. Employers and employees are encouraged to use interim solutions to enable employees to keep working as much as possible.

D.18. Federal agencies are required to have timelines in their written reasonable accommodation procedures governing how quickly they will process requests and provide reasonable accommodations. What happens if circumstances created by the pandemic prevent an agency from meeting this timeline? (9/8/20; adapted from 3/27/20 Webinar Question 19)

Situations created by the current COVID-19 crisis may constitute an “extenuating circumstance”—something beyond a Federal agency’s control—that may justify exceeding the normal timeline that an agency has adopted in its internal reasonable accommodation procedures.

E. Pandemic-Related Harassment Due to National Origin, Race, or Other Protected Characteristics

E.1. What practical tools are available to employers to reduce and address workplace harassment that may arise as a result of the COVID-19 pandemic? (4/9/20)

Employers can help reduce the chance of harassment by explicitly communicating to the workforce that fear of the COVID-19 pandemic should not be misdirected against individuals because of a protected characteristic, including their national origin, race, or other prohibited bases.

Practical anti-harassment tools provided by the EEOC for small businesses can be found here:

- Anti-harassment policy tips for small businesses
- Select Task Force on the Study of Harassment in the Workplace (includes detailed recommendations and tools to aid in designing effective anti-harassment policies; developing training curricula; implementing complaint, reporting, and investigation procedures; creating an organizational culture in which harassment is not tolerated):
  - report;
E.2. Are there steps an employer should take to address possible harassment and discrimination against coworkers when it re-opens the workplace? (4/17/20)

Yes. An employer may remind all employees that it is against the federal EEO laws to harass or otherwise discriminate against coworkers based on race, national origin, color, sex, religion, age (40 or over), disability, or genetic information. It may be particularly helpful for employers to advise supervisors and managers of their roles in watching for, stopping, and reporting any harassment or other discrimination. An employer may also make clear that it will immediately review any allegations of harassment or discrimination and take appropriate action.

E.3. How may employers respond to pandemic-related harassment, in particular against employees who are or are perceived to be Asian? (6/11/20)

Managers should be alert to demeaning, derogatory, or hostile remarks directed to employees who are or are perceived to be of Chinese or other Asian national origin, including about the coronavirus or its origins.

All employers covered by Title VII should ensure that management understands in advance how to recognize such harassment. Harassment may occur using electronic communication tools—regardless of whether employees are in the workplace, teleworking, or on leave—and also in person between employees at the worksite. Harassment of employees at the worksite may also originate with contractors, customers or clients, or, for example, with patients or their family members at health care facilities, assisted living facilities, and nursing homes. Managers should know their legal obligations and be instructed to quickly identify and resolve potential problems, before they rise to the level of unlawful discrimination.

Employers may choose to send a reminder to the entire workforce noting Title VII's prohibitions on harassment, reminding employees that harassment will not be tolerated, and inviting anyone who experiences or witnesses workplace harassment to report it to management. Employers may remind employees that harassment can result in disciplinary action up to and including termination.

E.4. An employer learns that an employee who is teleworking due to the pandemic is sending harassing emails to another worker. What actions should the employer take? (6/11/20)

The employer should take the same actions it would take if the employee was in the workplace. Employees may not harass other employees through, for example, emails, calls, or platforms for video or chat communication and collaboration.

F. Furloughs and Layoffs

F.1. Under the EEOC's laws, what waiver responsibilities apply when an employer is conducting layoffs? (4/9/20)

Special rules apply when an employer is offering employees severance packages in exchange for a general release of all discrimination claims against the employer. More information is available in EEOC's technical assistance document on severance agreements.
F.2. What are additional EEO considerations in planning furloughs or layoffs? (9/8/20; adapted from 3/27/20 Webinar Question 13)

The laws enforced by the EEOC prohibit covered employers from selecting people for furlough or layoff because of that individual’s race, color, religion, national origin, sex, age, disability, protected genetic information, or in retaliation for protected EEO activity.

G. Return to Work

G.1. As government stay-at-home orders and other restrictions are modified or lifted in your area, how will employers know what steps they can take consistent with the ADA to screen employees for COVID-19 when entering the workplace? (4/17/20)

The ADA permits employers to make disability-related inquiries and conduct medical exams if job-related and consistent with business necessity. Inquiries and reliable medical exams meet this standard if it is necessary to exclude employees with a medical condition that would pose a direct threat to health or safety.

Direct threat is to be determined based on the best available objective medical evidence. The guidance from CDC or other public health authorities is such evidence. Therefore, employers will be acting consistent with the ADA as long as any screening implemented is consistent with advice from the CDC and public health authorities for that type of workplace at that time.

For example, this may include continuing to take temperatures and asking questions about symptoms (or require self-reporting) of all those entering the workplace. Similarly, the CDC recently posted information on return by certain types of critical workers.

Employers should make sure not to engage in unlawful disparate treatment based on protected characteristics in decisions related to screening and exclusion.

G.2. An employer requires returning workers to wear personal protective gear and engage in infection control practices. Some employees ask for accommodations due to a need for modified protective gear. Must an employer grant these requests? (4/17/20)

An employer may require employees to wear protective gear (for example, masks and gloves) and observe infection control practices (for example, regular hand washing and social distancing protocols).

However, where an employee with a disability needs a related reasonable accommodation under the ADA (e.g., non-latex gloves, modified face masks for interpreters or others who communicate with an employee who uses lip reading, or gowns designed for individuals who use wheelchairs), or a religious accommodation under Title VII (such as modified equipment due to religious garb), the employer should discuss the request and provide the modification or an alternative if feasible and not an undue hardship on the operation of the employer’s business under the ADA or Title VII.

G.3. What does an employee need to do in order to request reasonable accommodation from her employer because she has one of the medical conditions that CDC says may put her at higher risk for severe illness from COVID-19? (5/5/20)

An employee—or a third party, such as an employee’s doctor—must let the employer know that she needs a change for a reason related to a medical condition (here, the underlying condition). Individuals may request
accommodation in conversation or in writing. While the employee (or third party) does not need to use the term “reasonable accommodation” or reference the ADA, she may do so.

The employee or her representative should communicate that she has a medical condition that necessitates a change to meet a medical need. After receiving a request, the employer may ask questions or seek medical documentation to help decide if the individual has a disability and if there is a reasonable accommodation, barring undue hardship, that can be provided.

**G.4. The CDC identifies a number of medical conditions that might place individuals at “higher risk for severe illness” if they get COVID-19. An employer knows that an employee has one of these conditions and is concerned that his health will be jeopardized upon returning to the workplace, but the employee has not requested accommodation. How does the ADA apply to this situation? (5/7/20)**

First, if the employee does not request a reasonable accommodation, the ADA does not mandate that the employer take action.

If the employer is concerned about the employee’s health being jeopardized upon returning to the workplace, the ADA does not allow the employer to exclude the employee—or take any other adverse action—solely because the employee has a disability that the CDC identifies as potentially placing him at “higher risk for severe illness” if he gets COVID-19. Under the ADA, such action is not allowed unless the employee’s disability poses a “direct threat” to his health that cannot be eliminated or reduced by reasonable accommodation.

The ADA direct threat requirement is a high standard. As an affirmative defense, direct threat requires an employer to show that the individual has a disability that poses a “significant risk of substantial harm” to his own health under 29 C.F.R. section 1630.2(r), (regulation addressing direct threat to health or safety of self or others). A direct threat assessment cannot be based solely on the condition being on the CDC’s list; the determination must be an individualized assessment based on a reasonable medical judgment about this employee’s disability—not the disability in general—using the most current medical knowledge and/or on the best available objective evidence. The ADA regulation requires an employer to consider the duration of the risk, the nature and severity of the potential harm, the likelihood that the potential harm will occur, and the imminence of the potential harm. Analysis of these factors will likely include considerations based on the severity of the pandemic in a particular area and the employee’s own health (for example, is the employee’s disability well-controlled), and his particular job duties. A determination of direct threat also would include the likelihood that an individual will be exposed to the virus at the worksite. Measures that an employer may be taking in general to protect all workers, such as mandatory social distancing, also would be relevant.

Even if an employer determines that an employee’s disability poses a direct threat to his own health, the employer still cannot exclude the employee from the workplace—or take any other adverse action—unless there is no way to provide a reasonable accommodation (absent undue hardship). The ADA regulations require an employer to consider whether there are reasonable accommodations that would eliminate or reduce the risk so that it would be safe for the employee to return to the workplace while still permitting performance of essential functions. This can involve an interactive process with the employee. If there are not accommodations that permit this, then an employer must consider accommodations such as telework, leave, or reassignment (perhaps to a different job in a place where it may be safer for the employee to work or that permits telework). An employer may only bar an employee from the workplace if, after going through all these steps, the facts support the conclusion that the employee poses a significant risk of substantial harm to himself that cannot be reduced or eliminated by reasonable accommodation.
G.5. What are examples of accommodation that, absent undue hardship, may eliminate (or reduce to an acceptable level) a direct threat to self? (5/5/20)

Accommodations may include additional or enhanced protective gowns, masks, gloves, or other gear beyond what the employer may generally provide to employees returning to its workplace. Accommodations also may include additional or enhanced protective measures, for example, erecting a barrier that provides separation between an employee with a disability and coworkers/the public or increasing the space between an employee with a disability and others. Another possible reasonable accommodation may be elimination or substitution of particular “marginal” functions (less critical or incidental job duties as distinguished from the “essential” functions of a particular position). In addition, accommodations may include temporary modification of work schedules (if that decreases contact with coworkers and/or the public when on duty or commuting) or moving the location of where one performs work (for example, moving a person to the end of a production line rather than in the middle of it if that provides more social distancing).

These are only a few ideas. Identifying an effective accommodation depends, among other things, on an employee’s job duties and the design of the workspace. An employer and employee should discuss possible ideas; the Job Accommodation Network (www.askjan.org) also may be able to assist in helping identify possible accommodations. As with all discussions of reasonable accommodation during this pandemic, employers and employees are encouraged to be creative and flexible.

G.6. As a best practice, and in advance of having some or all employees return to the workplace, are there ways for an employer to invite employees to request flexibility in work arrangements? (6/11/20)

Yes. The ADA and the Rehabilitation Act permit employers to make information available in advance to all employees about who to contact—if they wish—to request accommodation for a disability that they may need upon return to the workplace, even if no date has been announced for their return. If requests are received in advance, the employer may begin the interactive process. An employer may choose to include in such a notice all the CDC-listed medical conditions that may place people at higher risk of serious illness if they contract COVID-19, provide instructions about who to contact, and explain that the employer is willing to consider on a case-by-case basis any requests from employees who have these or other medical conditions.

An employer also may send a general notice to all employees who are designated for returning to the workplace, noting that the employer is willing to consider requests for accommodation or flexibilities on an individualized basis. The employer should specify if the contacts differ depending on the reason for the request – for example, if the office or person to contact is different for employees with disabilities or pregnant workers than for employees whose request is based on age or child-care responsibilities.

Either approach is consistent with the ADEA, the ADA, and the May 29, 2020 CDC guidance that emphasizes the importance of employers providing accommodations or flexibilities to employees who, due to age or certain medical conditions, are at higher risk for severe illness.

Regardless of the approach, however, employers should ensure that whoever receives inquiries knows how to handle them consistent with the different federal employment nondiscrimination laws that may apply, for instance, with respect to accommodations due to a medical condition, a religious belief, or pregnancy.

G.7. What should an employer do if an employee entering the worksite requests an alternative method of screening due to a medical condition? (6/11/20)

This is a request for reasonable accommodation, and an employer should proceed as it would for any other request for accommodation under the ADA or the Rehabilitation Act. If the requested change is easy to provide
and inexpensive, the employer might voluntarily choose to make it available to anyone who asks, without going through an interactive process. Alternatively, if the disability is not obvious or already known, an employer may ask the employee for information to establish that the condition is a disability and what specific limitations require an accommodation. If necessary, an employer also may request medical documentation to support the employee’s request, and then determine if that accommodation or an alternative effective accommodation can be provided, absent undue hardship.

Similarly, if an employee requested an alternative method of screening as a religious accommodation, the employer should determine if accommodation is available under Title VII.

H. Age

H.1. The CDC has explained that individuals age 65 and over are at higher risk for a severe case of COVID-19 if they contract the virus and therefore has encouraged employers to offer maximum flexibilities to this group. Do employees age 65 and over have protections under the federal employment discrimination laws? (6/11/20)

The Age Discrimination in Employment Act (ADEA) prohibits employment discrimination against individuals age 40 and older. The ADEA would prohibit a covered employer from involuntarily excluding an individual from the workplace based on his or her being 65 or older, even if the employer acted for benevolent reasons such as protecting the employee due to higher risk of severe illness from COVID-19.

Unlike the ADA, the ADEA does not include a right to reasonable accommodation for older workers due to age. However, employers are free to provide flexibility to workers age 65 and older; the ADEA does not prohibit this, even if it results in younger workers ages 40-64 being treated less favorably based on age in comparison.

Workers age 65 and older also may have medical conditions that bring them under the protection of the ADA as individuals with disabilities. As such, they may request reasonable accommodation for their disability as opposed to their age.

H.2. If an employer is choosing to offer flexibilities to other workers, may older comparable workers be treated less favorably based on age? (9/8/20; adapted from 3/27/20 Webinar Question 12)

No. If an employer is allowing other comparable workers to telework, it should make sure it is not treating older workers less favorably based on their age.

I. Caregivers/Family Responsibilities

I.1. If an employer provides telework, modified schedules, or other benefits to employees with school-age children due to school closures or distance learning during the pandemic, are there sex discrimination considerations? (6/11/20)

Employers may provide any flexibilities as long as they are not treating employees differently based on sex or other EEO-protected characteristics. For example, under Title VII, female employees cannot be given more favorable treatment than male employees because of a gender-based assumption about who may have caretaking responsibilities for children.
J. Pregnancy

J.1. Due to the pandemic, may an employer exclude an employee from the workplace involuntarily due to pregnancy? (6/11/20)

No. Sex discrimination under Title VII of the Civil Rights Act includes discrimination based on pregnancy. Even if motivated by benevolent concern, an employer is not permitted to single out workers on the basis of pregnancy for adverse employment actions, including involuntary leave, layoff, or furlough.

J.2. Is there a right to accommodation based on pregnancy during the pandemic? (6/11/20)

There are two federal employment discrimination laws that may trigger accommodation for employees based on pregnancy.

First, pregnancy-related medical conditions may themselves be disabilities under the ADA, even though pregnancy itself is not an ADA disability. If an employee makes a request for reasonable accommodation due to a pregnancy-related medical condition, the employer must consider it under the usual ADA rules.

Second, Title VII as amended by the Pregnancy Discrimination Act specifically requires that women affected by pregnancy, childbirth, and related medical conditions be treated the same as others who are similar in their ability or inability to work. This means that a pregnant employee may be entitled to job modifications, including telework, changes to work schedules or assignments, and leave to the extent provided for other employees who are similar in their ability or inability to work. Employers should ensure that supervisors, managers, and human resources personnel know how to handle such requests to avoid disparate treatment in violation of Title VII.
SARS-CoV-2 Testing Strategy: Considerations for Non-Healthcare Workplaces

Testing in Non-Healthcare Workplaces

Updated July 22, 2020

Note: This document provides guidance on the appropriate use of testing and does not dictate the determination of payment decisions or insurance coverage of such testing, except as may be otherwise referenced (or prescribed) by another entity or federal or state agency.

These interim considerations on SARS-CoV-2 testing strategies for non-healthcare workplaces during the COVID-19 pandemic are based on what is currently known about the transmission and severity of COVID-19 as of the date of posting, July 22, 2020.

The US Centers for Disease Control and Prevention (CDC) will update these considerations as needed and as additional information becomes available. Please check the CDC website periodically for updated interim guidance.

Purpose

The purpose of this document is to provide employers with strategies for consideration of incorporating testing for SARS-CoV-2, the virus that causes COVID-19, into a workplace COVID-19 preparedness, response, and control plan.

Employers are encouraged to collaborate with state, territorial, tribal and local health officials to determine whether and how to implement the following testing strategies and which one(s) would be most appropriate for their circumstances. These considerations are meant to supplement, not replace, any federal, state, local, territorial, or tribal health and safety laws, rules, and regulations with which workplaces must comply. These strategies should be carried out in a manner consistent with law and regulation, including laws protecting employee privacy and confidentiality. They should also be carried out consistent with Equal Employment Opportunity Commission guidance regarding permissible testing policies and procedures. Employers paying for testing of employees should put procedures in place for rapid notification of results and establish appropriate measures based on testing results including instructions regarding self-isolation and restrictions on workplace access.

Considerations for use of a strategy to test for SARS-CoV-2 infection

SARS-CoV-2 testing may be incorporated as part of a comprehensive approach to reducing transmission in non-healthcare workplaces. Symptom screening, testing, and contact tracing [58 pages] are strategies to identify workers infected with SARS-CoV-2, the virus that causes COVID-19, so that actions can be taken to slow and stop the spread of the virus.

Employees undergoing testing should receive clear information on:

- the manufacturer and name of the test, the type of test, the purpose of the test, the reliability of the test, any limitations associated with the test, who will pay for the test, and how the test will be performed, and
- how to understand what the results mean, actions associated with negative or positive results, who will receive the results, how the results may be used, and any consequences for declining to be tested.
Individuals tested are required to receive patient fact sheets as part of the test’s emergency use authorization.

The Occupational Safety and Health Administration has issued interim guidance for enforcing the requirements of 29 CFR Part 1904 with respect to the recording of occupational illnesses, specifically cases of COVID-19. Under OSHA’s recordkeeping requirements, COVID-19 is a recordable illness, and thus employers are responsible for recording cases of COVID-19, if the case meets certain requirements. Employers are encouraged to frequently check OSHA’s webpage at www.osha.gov/coronavirus for updates.

Testing for SARS-CoV-2 infection

Viral tests approved or authorized by the Food and Drug Administration (FDA) are used to diagnose current infection with SARS-CoV-2, the virus that causes COVID-19. Viral tests evaluate whether the virus is present in respiratory or other samples. Results from these tests help public health officials identify and isolate people who are infected in order to minimize SARS-CoV-2 transmission.

Antibody tests approved or authorized by the FDA are used to detect past infection with SARS-CoV-2. CDC does not currently recommend using antibody testing as the sole basis for diagnosing current infection. Depending on when someone was infected and the timing of the test, the test may not find antibodies in someone with a current SARS-CoV-2 infection. In addition, it is currently not known whether a positive antibody test indicates immunity against SARS-CoV-2; therefore, antibody tests should not be used at this time to determine if an individual is immune.

Categories for SARS-CoV-2 testing

CDC describes strategies for SARS-CoV-2 viral testing for five categories of people:

- Testing individuals with signs or symptoms consistent with COVID-19
- Testing asymptomatic individuals with recent known or suspected exposure to SARS-CoV-2 to control transmission
- Testing asymptomatic individuals without known or suspected exposure to SARS-CoV-2 for early identification in special settings
- Testing to determine resolution of infection (e.g., discontinuation of home isolation)
- Public health surveillance for SARS-CoV-2

Testing individuals with signs or symptoms consistent with COVID-19

Employers may consider conducting daily in-person or virtual health checks (e.g., symptom and/or temperature screening) to identify employees with signs or symptoms consistent with COVID-19 before they enter a facility, in accordance with CDC’s General Business FAQs. Employers should follow guidance from the Equal Employment Opportunity Commission regarding confidentiality of medical records from health checks.

Workers with COVID-19 symptoms should be immediately separated from other employees, customers, and visitors, and sent home or to a healthcare facility, depending on how severe their symptoms are, and follow CDC guidance for caring for oneself. To prevent stigma and discrimination in the workplace, make employee health screenings as private as possible. Consistent with CDC’s recommendations, workers with COVID-19 symptoms should be referred to a healthcare provider for evaluation and potential testing. Waiting for test results prior to returning to work is preferred to keep potentially infected workers out of the workplace.

Employers are encouraged to implement flexible sick leave and supportive policies and practices as part of a comprehensive approach to prevent and reduce transmission among employees. The Families First Coronavirus Response Act (FFCRA or Act) requires certain employers to provide their employees with paid sick leave or expanded family and medical leave for specified reasons related to COVID-19. Employers with fewer than 500 employees are eligible for 100% tax credits for Families First Coronavirus Response Act COVID-19 paid leave provided through December 31, 2020, up to certain limits.

Positive test results using a viral test indicate that the employee has COVID-19 and should not come to work and should isolate at home. Decisions to discontinue home isolation for workers with COVID-19 and allow them to return to work may follow either a symptom-based, time based, or a test-based strategy (see Testing to determine resolution of infection below).
Testing asymptomatic individuals with recent known or suspected exposure to SARS-CoV-2 to control transmission

Case investigation is typically initiated when a health department receives a report from a laboratory of a positive SARS-CoV-2 viral test result or a report from a healthcare provider of a patient with a confirmed or probable diagnosis of COVID-19.

Viral testing may be recommended for close contacts of persons with COVID-19 in jurisdictions with testing capacity. Because of the potential for asymptomatic and pre-symptomatic transmission of SARS-CoV-2, it is important that individuals exposed to people with known or suspected COVID-19 be quickly identified and quarantined. Viral testing can detect if these individuals are currently infected. The health department may reach out to the employer for assistance in identifying close contacts of the worker as well as possible contacts. Employers are encouraged to work with public health departments investigating cases of COVID-19 and tracing contacts to help reduce the spread of SARS-CoV-2 in their workplaces and communities.

Because there may be a delay between the time a person is exposed to the virus and the time that virus can be detected by testing, early testing after exposure at a single time point may miss many infections. Testing that is repeated at different points in time, also referred to as serial testing, may be more likely to detect infection among close contacts of a COVID-19 case than testing done at a single point in time.

Even if close contacts are monitored with serial testing, it is critical that they strictly adhere to other preventive measures including social distancing, wearing cloth face coverings for source control if the hazard assessment has determined that they do not require personal protective equipment such as a respirator or medical facemask for protection, and practicing hand hygiene.

Testing may also be considered for possible close contacts of persons diagnosed with COVID-19 in collaboration with the local health department if resources permit. A risk-based approach to testing possible contacts of a person with confirmed COVID-19 may be applied. Such an approach should take into consideration the likelihood of exposure, which is affected by the characteristics of the workplace and the results of contact investigations. In some settings, broader testing (i.e., testing beyond individually identified close contacts to those who are possible close contacts), such as targeting workers who worked in the same area and during the same shift, may be considered as part of a strategy to control the transmission of SARS-CoV-2 in the workplace. The rationale is that identification of contacts may be imprecise. High-risk settings that have demonstrated potential for rapid and widespread dissemination of SARS-CoV-2 include:

- High-density critical infrastructure workplaces
- Workplaces where employees live in congregate settings (e.g., fishing vessels, offshore oil platforms, farmworker housing or wildland firefighter camps)
- Workplaces with populations at risk for severe illness if they are infected, such as nursing homes

Employers are encouraged to consult with state, local, territorial, and tribal health departments to help inform decision-making about broad-based testing.

If employees are tested after close contact or possible close contact with someone who has a confirmed or probable diagnosis of COVID-19, care should be taken to inform these employees of their possible exposure to SARS-CoV-2 in the workplace while maintaining confidentiality of the individual with COVID-19, as required by the Americans with Disabilities Act (ADA) and consistent with the U.S. Equal Employment Opportunity Commission (EEOC) guidance regarding What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws.

Testing asymptomatic individuals without known or suspected exposure to SARS-CoV-2 for early identification in special settings

Viral testing of workers without symptoms may be useful to detect COVID-19 early and stop transmission quickly, particularly in areas with moderate to substantial community transmission. When communities experience moderate to substantial transmission, workplace settings for which these approaches may be considered include:

- Workplaces where physical distancing is difficult and workers are in close contact (within 6 feet for 15 minutes or more) with co-workers or the public
- Workplaces in remote settings where medical evaluation or treatment may be delayed
• Workplaces where continuity of operations is a high priority (e.g., critical infrastructure sectors)
• Workplaces providing congregate housing for employees (e.g., fishing vessels, offshore oil platforms, farmworker housing or wildland firefighter camps)

Approaches may include initial testing of all workers before entering a workplace, periodic testing of workers at regular intervals, and/or targeted testing of new workers or those returning from a prolonged absence. Several factors may be helpful in determining the interval for periodic testing including:

• The availability of testing
• The latency between exposure and development of a positive SARS-CoV-2 viral test
• Businesses that fall into one of the workplace categories described above
• The rate or change in rate of people getting infected in the surrounding community
• How many employees tested positive during previous rounds of testing
• Your relevant experience with workplace outbreaks

State, local, territorial, and tribal health departments may be able to provide assistance on any local context or guidance impacting the workplace. Before testing a large proportion of asymptomatic workers without known or suspected exposure, employers are encouraged to have a plan in place for how they will modify operations based on test results and manage a higher risk of false positive results in a low prevalence population.

Testing to determine resolution of infection

The decision to end home isolation and return to work for employees with suspected or confirmed SARS-CoV-2 infection should be made in the context of clinical and local circumstances. Polymerase chain reaction (PCR) amplification tests have detected SARS-CoV-2 RNA in some people’s respiratory samples after they have recovered from COVID-19. Prolonged viral shedding has been demonstrated without direct evidence for virus capable of replicating or causing infection. Consequently, in most cases, evidence supports a symptom-based strategy to determine when to discontinue home isolation or precautions. For persons who are severely immunocompromised, a test-based strategy could be considered in consultation with infectious diseases experts. For all others, a test-based strategy is no longer recommended except to discontinue isolation or precautions earlier than would occur under the symptom-based strategy.

Under the Americans with Disabilities Act, employers are permitted to require a healthcare provider’s note to verify that employees are healthy and able to return to work. However, as a practical matter, employers should be aware that healthcare provider offices and medical facilities may be extremely busy during periods of community transmission of SARS-CoV-2 and may not be able to provide such documentation in a timely manner. In such cases, employers should consider not requiring a healthcare provider’s note for employees who are sick to validate their illness, qualify for sick leave, or to return to work. Most people with COVID-19 have mild illness, can recover at home without medical care, and can follow CDC recommendations to determine when to discontinue home isolation and return to work.

Public health surveillance for SARS-CoV-2

Testing is considered to be surveillance when conducted to detect transmission hot spots, or to better understand disease trends in a workplace. These goals are consistent with employer-based occupational medicine surveillance programs. Occupational medicine surveillance programs may use testing to assess the burden of SARS-CoV-2 in the workforce, assess factors that place employees at risk for workplace acquisition of SARS-CoV-2, or evaluate the effectiveness of workplace infection control programs. Surveillance should only be undertaken if the results have a reasonable likelihood of benefitting workers.

Footnote

1. The rate of false negative nucleic acid tests, a type of viral test, after exposure have been reported as: day 1: 100%; day 4: 67%; day 5: 38%; day 8: 20%; day 9: 21%; and then rising to 66% on day 21. See: https://www.acpjournals.org/doi/full/10.7326/M20-1495

Last Updated July 22, 2020
Enforcement Memos / Revised Enforcement Guidance for Recording Cases of Coronavirus Disease 2019 (COVID-19)

May 19, 2020

MEMORANDUM FOR:
REGIONAL ADMINISTRATORS
STATE PLAN DESIGNEES

THROUGH:
AMANDA EDENS
Deputy Assistant Secretary

FROM:
LEE ANNE JILLINGS, Acting Director
Directorate of Technical Support and Emergency Management

PATRICK J. KAPUST, Acting Director
Directorate of Enforcement Programs

SUBJECT:
Revised Enforcement Guidance for Recording Cases of Coronavirus Disease 2019 (COVID-19)

This memorandum provides updated interim guidance to Compliance Safety and Health Officers (CSHOs) for enforcing the requirements of 29 CFR Part 1904 with respect to the recording of occupational illnesses, specifically cases of COVID-19. On May 26, 2020, the previous memorandum on this topic[1] will be rescinded, and this new memorandum will go into and remain in effect until further notice. This guidance is intended to be time-limited to the current COVID-19 public health crisis. Please frequently check OSHA's webpage at www.osha.gov/coronavirus for updates.

Under OSHA’s recordkeeping requirements, COVID-19 is a recordable illness, and thus employers are responsible for recording cases of COVID-19, if:

1. The case is a confirmed case of COVID-19, as defined by the Centers for Disease Control and Prevention (CDC);[2]
2. The case is work-related as defined by 29 CFR § 1904.5,[3] and
3. The case involves one or more of the general recording criteria set forth in 29 CFR § 1904.7.[4]

Confirmed cases of COVID-19 have now been found in nearly all parts of the country, and outbreaks among workers in industries other than healthcare, emergency response, or correctional institutions have been identified. As transmission and prevention of infection have become better understood, both the government and the private sector have taken rapid and evolving steps to slow the virus's spread, protect employees, and adapt to new ways of doing business. As the virus's spread now slows in certain areas of the country, states are taking steps to reopen their economies and workers are returning to their workplaces. All these facts—incidence, adaptation, and the return of the workforce—indicate that employers should be taking action to determine whether employee COVID-19 illnesses are work-related and thus recordable. Given the nature of the disease and ubiquity of community spread, however, in many instances it remains difficult to determine whether a COVID-19 illness is work-related, especially when an employee has experienced potential exposure both in and out of the workplace.

In light of these considerations, OSHA is exercising its enforcement discretion in order to provide certainty to employers and workers. Accordingly, until further notice, OSHA will enforce the recordkeeping requirements of 29 CFR 1904 for employee COVID-19 illnesses for all employers according to the guidelines below. Recording a COVID-19 illness does not, of itself, mean that the employer has violated any OSHA standard. And pursuant to existing regulations, employers with 10 or fewer employees and certain employers in low hazard industries have no recording obligations; they need only report work-related COVID-19 illnesses that result in a fatality or an employee's in-patient hospitalization, amputation, or loss of an eye.[5]

* * *

Because of the difficulty with determining work-relatedness, OSHA is exercising enforcement discretion to assess employers' efforts in making work-related determinations.

In determining whether an employer has complied with this obligation and made a reasonable determination of work-relatedness, CSHOs should apply the following considerations:
- The reasonableness of the employer's investigation into work-relatedness. Employers, especially small employers, should not be expected to undertake extensive medical inquiries, given employee privacy concerns and most employers' lack of expertise in this area. It is sufficient in most circumstances for the employer, when it learns of an employee's COVID-19 illness, (1) to ask the employee how he believes he contracted the COVID-19 illness; (2) while respecting employee privacy, discuss with the employee his work and out-of-work activities that may have led to the COVID-19 illness; and (3) review the employee's work environment for potential SARS-CoV-2 exposure. The review in (3) should be informed by any other instances of workers in that environment contracting COVID-19 illness.

- The evidence available to the employer. The evidence that a COVID-19 illness was work-related should be considered based on the information reasonably available to the employer at the time it made its work-relatedness determination. If the employer later learns more information related to an employee's COVID-19 illness, then that information should be taken into account as well in determining whether an employer made a reasonable work-relatedness determination.

- The evidence that a COVID-19 illness was contracted at work. CSHOs should take into account all reasonably available evidence, in the manner described above, to determine whether an employer has complied with its recording obligation. This cannot be reduced to a ready formula, but certain types of evidence may weigh in favor of or against work-relatedness. For instance:
  - COVID-19 illnesses are likely work-related when several cases develop among workers who work closely together and there is no alternative explanation.
  - An employee's COVID-19 illness is likely work-related if it is contracted shortly after lengthy, close exposure to a particular customer or coworker who has a confirmed case of COVID-19 and there is no alternative explanation.
  - An employee's COVID-19 illness is likely work-related if his job duties include having frequent, close exposure to the general public in a locality with ongoing community transmission and there is no alternative explanation.
  - An employee's COVID-19 illness is likely not work-related if she is the only worker to contract COVID-19 in her vicinity and her job duties do not include having frequent contact with the general public, regardless of the rate of community spread.
  - An employee's COVID-19 illness is likely not work-related if he, outside the workplace, closely and frequently associates with someone (e.g., a family member, significant other, or close friend) who (1) has COVID-19; (2) is not a coworker, and (3) exposes the employee during the period in which the individual is likely infectious.
  - CSHOs should give due weight to any evidence of causation, pertaining to the employee illness, at issue provided by medical providers, public health authorities, or the employee herself.

If, after the reasonable and good faith inquiry described above, the employer cannot determine whether it is more likely than not that exposure in the workplace played a causal role with respect to a particular case of COVID-19, the employer does not need to record that COVID-19 illness. In all events, it is important as a matter of worker health and safety, as well as public health, for an employer to examine COVID-19 cases among workers and respond appropriately to protect workers, regardless of whether a case is ultimately determined to be work-related.

CSHOs will generally refer to CPL 02-00-135, Recordkeeping Policies and Procedures Manual (Dec. 30, 2004),[6] and CPL 02-00-163, Field Operations Manual (Sept. 13, 2019),[7] Chapters 3 and 6, as applicable. The following additional specific enforcement guidance is provided for CSHOs:

- COVID-19 is a respiratory illness and should be coded as such on the OSHA Form 300. Because this is an illness, if an employee voluntarily requests that his or her name not be entered on the log, the employer must comply as specified under 29 CFR § 1904.29(b)(7)(vi).

If you have any questions regarding this policy, please contact Elizabeth Grossman, Director of the Office of Statistical Analysis, at (202) 693-2225.

cc: DCSP
 DSG


[3] Under 29 CFR § 1904.5, an employer must consider an injury or illness to be work-related if an event or exposure in the work environment (as defined by 29 CFR § 1904.5(b)(1)) either caused or contributed to the resulting condition or significantly aggravated a pre-existing injury or illness. Work-relatedness is presumed for injuries and illnesses resulting from events or exposures occurring in the work environment, unless an exception in 29 CFR § 1904.5(b)(2) specifically applies. See www.osha.gov/lawsregs/regulations/standardnumber/1904/1904.5. As discussed below, OSHA is exercising enforcement discretion regarding work-relatedness in the context of employee COVID-19 illness. Back to text
[4] Under 29 CFR § 1904.7, an employer must consider an injury or illness to meet the general recording criteria, and therefore to be recordable, if it results in any of the following: death, days away from work, restricted work or transfer to another job, medical treatment beyond first aid, or loss of consciousness. An employer must also consider a case to meet the general recording criteria if it involves a significant injury or illness diagnosed by a physician or other licensed health care professional, even if it does not result in death, days away from work, restricted work or job transfer, medical treatment beyond first aid, or loss of consciousness. See www.osha.gov/laws-regulations/standardnumber/1904/1904.7. Back to text


Privacy during coronavirus

Elisa Jillson
Jun 19, 2020

During this pandemic, preserving public health has, rightly, been our nation’s top concern. But a lively debate has arisen during this time about whether that top priority necessarily means that other values – such as privacy – need to give way. If tracking people’s location will facilitate contact tracing and enforcement of shelter-in-place mandates, do we give governments and commercial partners carte blanche to track our whereabouts?

Will enforcing longstanding privacy requirements impede the flow of life-saving public health information?

Fortunately, we do not live in a zero-sum game, where we must choose either our health or our privacy. Indeed, as the nation’s primary privacy enforcement agency, the FTC has long struck a balance between protecting consumer privacy while facilitating information flows. And, during the pandemic, the FTC has continued in this role, such as by providing:

- Guidance to ed tech providers, schools, and parents about navigating privacy and security issues;
- Advice for businesses and consumers about how to safely use videoconference services (our new way of connecting) in a way that protects privacy; and
- Tips on how to use artificial intelligence technology (which can be a tool for targeting public health resources) in a fair and non-discriminatory manner.

If your business is looking to leverage consumer data to do your part in this crisis, we offer these tips on how to provide these services in a privacy protective way:

**Consider privacy and security as you’re developing your products and services, and not after launch.**

We’ve brought cases against start-ups, most recently against smart-lock manufacturer Tapplock, for rushing to get a product to market without considering privacy and security issues. Although we will be flexible and reasonable when it comes to bringing enforcement actions against companies engaged in good faith, thoughtful efforts to address the effects of the pandemic, it doesn’t pay to be in the news for privacy and security problems, and then have to retreat to address them.

**Use privacy protective technologies.**

There are many engineering tools that can preserve consumer privacy while getting the data you need to combat the coronavirus. For instance, researchers have developed privacy-friendly, decentralized protocols that allow users to voluntarily share encrypted data directly with epidemiologists.

**Consider using anonymous, aggregate data.**

Using anonymous, aggregate location data for public health purposes will allow you to sidestep many of the privacy concerns related to tracking individuals’ location. For example, if a consumer has granted you permission to use their location data, nothing would prohibit you from disclosing a heat map of average distances travelled for public health purposes. A consumer’s consent for this use of aggregate, anonymous data would not be required.

**Delete data when the crisis is over.**

If you tell consumers you’re collecting, analyzing, using, or sharing information for emergency public health purposes, only use it for those purposes, and delete the data when the need is over. This idea of “purpose limitation” or “use limitation” has been a standard tenet of privacy norms over the
years. And it also forms the basis of an allegation we made in our 2019 Facebook complaint, where we alleged that the company violated the FTC Act by claiming that it collected users' phone numbers for a consumer-protective security purpose, but used the information for advertising as well.

Navigating this crisis is requiring our resilience, patience, and strength. Navigating the crisis while also preserving values that we cherish – like privacy – is doable, with a bit of creativity and forethought.
July 28, 2020

The Honorable Mitch McConnell  
Majority Leader  
United States Senate  
Washington, DC 20510

The Honorable Charles Schumer  
Minority Leader  
United States Senate  
Washington, DC 20510

The Honorable Lamar Alexander  
Chairman  
Committee on Health, Education, Labor & Pensions  
Washington, DC 20510

The Honorable Patty Murray  
Ranking Member  
Committee on Health, Education, Labor & Pensions  
Washington, DC 20510

Dear Leader McConnell, Leader Schumer, Chairman Alexander, and Ranking Member Murray,

As you begin negotiations on another coronavirus stimulus package, we write to urge inclusion of commonsense privacy protections for COVID health data. Building public trust in COVID screening tools will be essential to ensuring meaningful participation in such efforts. With research consistently showing that Americans are reluctant to adopt COVID screening and tracing apps due to privacy concerns¹, the lack of health privacy protections could significantly undermine efforts to contain this virus and begin to safely re-open – particularly with many screening tools requiring a critical mass in order to provide meaningful benefits. According to one survey, 84% of Americans “fear that data collection efforts aimed at helping to contain the coronavirus cost too much in the way of privacy.”²

Public health experts have consistently pointed to health screening and contact tracing as essential elements of a comprehensive strategy to contain and eradicate COVID. Since the onset of the pandemic, employers, public venue operators, and consumer service providers have introduced a range of tools and resources to engage in symptom monitoring, contact tracing, exposure notification, temperature checks, and location tracking.³ Increasingly, we have seen


higher education institutions mandate the use of these applications for incoming students⁴ and employers mandate participation in these programs among employees.⁵

Health data is among the most sensitive data imaginable and even before this public health emergency, there has been increasing bipartisan concern with gaps in our nation’s health privacy laws. While a comprehensive update of health privacy protections is unrealistic at this time, targeted reforms to protect health data – particularly with clear evidence that a lack of privacy protections has inhibited public participation in screening activities – is both appropriate and necessary.

Our legislation does not prohibit or otherwise prevent employers, service providers, or any other entity from introducing COVID screening tools. Rather, it provides commonsense and widely understood rules related to the collection, retention, and usage of that information – most notably, stipulating that sensitive data collected under the auspices of efforts to contain COVID should not be used for unrelated purposes. As a litany of investigative reports, Congressional hearings, and studies have increasingly demonstrated, the widespread secondary use of Americans’ data – including sensitive health and geolocation data – has become a significant public concern. The legislation also ensures that Americans cannot be discriminated against on the basis of COVID health data – something particularly important given the disproportionate impact of this pandemic on communities of color.

Efforts by public health agencies to combat COVID-19, such as manual contract tracing, health screenings, interviews, and case investigations, are not restricted by our bill. And the legislation would allow for the collection, use, and sharing of data for public health research purposes and makes clear that it does not restrict use of health information for public health or other scientific research associated with a public health emergency.

Our urgent and forceful response to COVID-19 can coexist with protecting and even bolstering our health privacy. If not appropriately addressed, these issues could lead to a breakdown in public trust that could ultimately thwart successful public health surveillance initiatives. Privacy experts, patient advocates, civil rights leaders, and public interest organizations have resoundingly called for strong privacy protections to govern technological measures offered in

response to the COVID-19 crisis. In the absence of a federal privacy framework, experts and enforcers – including the Director of the Bureau of Consumer Protection of Federal Trade Commission – have encouraged targeted rules on this sensitive health data. The Public Health Emergency Privacy Act meets the needs raised by privacy and public health communities, and has been resoundingly endorsed by experts and civil society groups.

Providing Americans with assurance that their sensitive health data will not be misused will give Americans more confidence to participate in COVID screening efforts, strengthening our common mission in containing and eradicating COVID-19. For this reason, we urge you to include the privacy protections contained in the Public Health Emergency Privacy Act in any forthcoming stimulus package.

Thank you for your attention to this important matter.

Sincerely,

/s/ Mark R. Warner

Mark R. Warner
United States Senate

/s/ Richard Blumenthal

Richard Blumenthal
United States Senate

/s/ Michael F. Bennet

Michael F. Bennet
United States Senate

/s/ Mazie K. Hirono

Mazie K. Hirono
United States Senate

/s/ Angus S. King, Jr.

Angus S. King, Jr.
United States Senate

/s/ Robert Menendez

Robert Menendez
United States Senate

---


<table>
<thead>
<tr>
<th>/s/ Kamala D. Harris</th>
<th>/s/ Edward J. Markey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kamala D. Harris</td>
<td>Edward J. Markey</td>
</tr>
<tr>
<td>United States Senate</td>
<td>United States Senate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>/s/ Cory Booker</th>
<th>/s/ Tammy Baldwin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cory Booker</td>
<td>Tammy Baldwin</td>
</tr>
<tr>
<td>United States Senate</td>
<td>United States Senate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>/s/ Elizabeth Warren</th>
<th>/s/ Amy Klobuchar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elizabeth Warren</td>
<td>Amy Klobuchar</td>
</tr>
<tr>
<td>United States Senate</td>
<td>United States Senate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>/s/ Dick Durbin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Richard J. Durbin</td>
</tr>
<tr>
<td>United States Senate</td>
</tr>
</tbody>
</table>
116TH CONGRESS
2d SESSION

S. 3663

To protect the privacy of consumers' personal health information, proximity data, device data, and geolocation data during the coronavirus public health crisis.

IN THE SENATE OF THE UNITED STATES

MAY 7, 2020

Mr. WICKER (for himself, Mr. THUNE, Mr. MORAN, Mrs. BLACKBURN, and Mrs. FISCHER) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To protect the privacy of consumers' personal health information, proximity data, device data, and geolocation data during the coronavirus public health crisis.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “COVID–19 Consumer Data Protection Act of 2020”.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGGREGATED DATA.—The term “aggregated data” means information that—

(A) relates to a group or category of individuals; and

(B) does not identify, and is not linked or reasonably linkable to, any individual.

(2) AFFIRMATIVE EXPRESS CONSENT.—

(A) IN GENERAL.—The term “affirmative express consent” means an affirmative act by an individual that—

(i) clearly communicates the individual's authorization of an act or practice; and

(ii) is taken after the individual has been presented with a clear and conspicuous description of such act or practice.

(B) NO INFERENCE FROM INACTION.—For purposes of subparagraph (A), the affirmative express consent of an individual cannot be inferred from inaction.

(3) BUSINESS CONTACT INFORMATION.—The term “business contact information” means information related to an individual’s business position name or title, business telephone number, business address, business email address,
and other similar business information, provided that such information is collected, processed, or transferred solely for purposes related to such individual’s professional activities.

(4) COLLECTION.—The term “collection” means buying, renting, gathering, accessing, or otherwise acquiring any covered data of an individual by any means.

(5) COMMISSION.—The term “Commission” means the Federal Trade Commission.

(6) COVERED DATA.—
   (A) IN GENERAL.—The term “covered data” means precise geolocation data, proximity data, a persistent identifier, and personal health information.
   (B) EXCLUSIONS.—Such term does not include the following:
      (i) Aggregated data.
      (ii) Business contact information.
      (iii) De-identified data.
      (iv) Employee screening data.
      (v) Publicly available information.

(7) COVERED ENTITY.—The term “covered entity” means, with respect to a set of covered data, any entity or person that—
   (A) is—
      (i) subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.); or
      (ii) a common carrier or nonprofit organization described in section 4(a)(4);
   (B) collects, processes, or transfers such covered data, or determines the means and purposes for the collection, processing, or transfer of covered data; and
   (C) is not a service provider with respect to such data.

(8) COVID–19 PUBLIC HEALTH EMERGENCY.—The term “COVID–19 public health emergency” means the period—
   (A) beginning on the date of enactment of this Act; and
   (B) ending on the last day of the public health emergency declared by the Secretary of Health and Human Services pursuant to section 319 of the Public Health Service Act (42 U.S.C. 247d) on January 31, 2020, entitled “Determination that a Public Health Emergency Exists Nationwide as the Result of the 2019 Novel Coronavirus” (including any renewal of such declaration pursuant to such section 319).

(9) DE-IDENTIFIED DATA.—The term “de-identified data” means information held by a covered entity that—
   (A) does not identify and is not reasonably linkable to an individual;
   (B) does not contain any personal identifiers or other information that could be readily used to re-identify the individual to whom the information pertains;
   (C) is subject to a public commitment by the covered entity—
      (i) to refrain from attempting to use such information to identify any individual; and
      (ii) to adopt technical and organizational measures to ensure that such information is not linked to any individual; and
   (D) is not disclosed by the covered entity to any other party unless the disclosure is subject to a contractually or other legally binding requirement that—
      (i) the recipient of the information shall not use the information to identify any individual; and
      (ii) all onward disclosures of the information shall be subject to the requirement described in clause (i).

(10) EMPLOYEE SCREENING DATA.—The term “employee screening data” means, with respect to a covered entity, covered data of an individual who is an employee, owner, director, officer, staff member, trainee, vendor, visitor, intern, volunteer, or contractor of the covered entity, provided that such data is only collected, processed, or transferred by the covered entity for the purpose of determining, for purposes related to the COVID–19 public health emergency, whether the individual is permitted to enter a physical site of operation of the covered entity.

(11) DELETE.—The term “delete” means to remove or destroy information such that it is not maintained in human or machine readable form and cannot be retrieved or utilized in the normal course of business.

(12) INDIVIDUAL.—
   (A) IN GENERAL.—The term “individual” means a natural person residing in the United States.
(B) EXCLUSION.—Such term does not include, with respect to a covered entity, an individual acting as a full-time or part-time, paid or unpaid employee, owner, director, officer, staff member, trainee, vendor, visitor, intern, volunteer, or contractor of a covered entity permitted to enter a physical site of operation of the covered entity.

(13) PERSISTENT IDENTIFIER.—The term “persistent identifier” means a technologically derived identifier that identifies an individual, or is linked or reasonably linkable to an individual over time and across services and platforms, which may include a customer number held in a cookie, a static Internet Protocol (IP) address, a processor or device serial number, or another unique device identifier.

(14) PERSONAL HEALTH INFORMATION.—

(A) IN GENERAL.—The term “personal health information” means information relating to an individual that

(i) is—

(I) genetic information of the individual; or

(II) information relating to the diagnosis or treatment of past, present, or future physical, mental health, or disability of the individual; and

(ii) identifies, or is reasonably linkable to, the individual.

(B) EXCLUSIONS.—Such term does not include the following:

(i) Information from education records that are subject to the requirements of section 444 of the General Education Provisions Act (20 U.S.C. 1232g, commonly referred to as the “Family Educational Rights and Privacy Act of 1974”) or from records described in subsection (a)(4)(B)(iv) of such section.

(ii) Information subject to regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note).

(15) PRECISE GEOLOCATION DATA.—The term “precise geolocation data” means technologically derived information capable of determining with reasonable specificity the past or present actual physical location of an individual at a specific point in time.

(16) PROCESS.—The term “process” means any operation or set of operations performed on covered data, including analyzing, organizing, structuring, retaining, using, or otherwise handling such data.

(17) PROXIMITY DATA.—The term “proximity data” means technologically derived information that identifies the past or present proximity of one individual to another.

(18) PUBLICLY AVAILABLE INFORMATION.—The term “publicly available information” means any information that

(A) has been lawfully made available to the general public from Federal, State, or local government records; or

(B) is widely available to the general public, including information from—

(i) a telephone book or online directory;

(ii) video, internet, or audio content; or

(iii) the news media or a website that is available to the general public on an unrestricted basis (for purposes of this subclause a website is not restricted solely because there is a fee or log-in requirement associated with accessing the website).

(19) SERVICE PROVIDER.—The term “service provider” means, with respect to a set of covered data, an entity that processes or transfers such covered data for the purpose of performing one or more services or functions on behalf of, and at the direction of, a covered entity to which it is not related.

(20) TRANSFER.—The term “transfer” means to disclose, release, share, disseminate, or otherwise make available covered data by any means.

SEC. 3. PRIVACY OF COVERED DATA.

(a) IN GENERAL.—During the COVID–19 public health emergency, it shall be unlawful for a covered entity to collect, process, or transfer the covered data of an individual for a purpose described in subsection (b) unless—

(1) the covered entity provides the individual with prior notice of the purpose for such collection, processing, or transfer;

(2) the individual has given affirmative express consent to such collection, processing, or transfer; and

(3) the covered entity publicly commits not to collect, process, or transfer such covered data for a purpose other than the purpose described in subsection (b) to which the individual consented unless—
(A) such collection, processing, or transfer is necessary to comply with the provisions of this Act or other applicable laws;

(B) such collection, processing, or transfer is necessary to carry out operational or administrative tasks in support of a purpose described in subsection (b) to which the individual has consented; or

(C) the individual gives affirmative express consent to such collection, processing, or transfer.

(b) Covered Purposes.—The purposes described in this subsection are the following:

(1) Collecting, processing, or transferring the covered data of an individual to track the spread, signs, or symptoms of COVID–19.

(2) Collecting, processing, or transferring the covered data of an individual to measure compliance with social distancing guidelines or other requirements related to COVID–19 that are imposed on individuals under a Federal, State, or local government order.

(3) Collecting, processing, or transferring the covered data of an individual to conduct contact tracing for COVID–19 cases.

(c) Transparency.—

(1) 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—

(A) 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;

(B) is made available in a clear and conspicuous manner to the public;

(C) 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;

(D) 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

(E) includes a general description of the covered entity’s data security practices.

(2) Reporting.—During the COVID–19 public health emergency, a covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall issue a public report not later than 30 days after the enactment of this Act and not less frequently than once every 60 days thereafter—

(A) stating in aggregate terms the number of individuals whose covered data the entity has collected, processed, or transferred for such a purpose; and

(B) describing the categories of covered data collected, processed, or transferred by the entity, the specific purposes for which each such category of covered data is collected, processed, or transferred, and, in the case of transferred covered data, to whom such data was transferred.

(d) Right to Opt-Out.—During the COVID–19 public health emergency, each covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall do the following:

(1) The covered entity shall provide an effective mechanism for an individual who has consented pursuant to subsection (a) to the collection, processing, or transfer of the individual's covered data for such a purpose to revoke such consent.

(2) A covered entity that receives a revocation of consent from an individual described in paragraph (1) shall, as soon as practicable but in no case later than 14 days after receiving such revocation, stop collecting, processing, or transferring the covered data of such individual for a purpose described in subsection (b), or shall de-identify all such data.

(e) Data Deletion.—A covered entity shall delete or de-identify all covered data collected, processed, or transferred for a purpose described in subsection (b) when it is no longer being used for such purpose and is no longer necessary to comply with a Federal, State, or local legal obligation, or the establishment, exercise, or defense of a legal claim.

(f) Data Accuracy.—A covered entity shall take reasonable measures to ensure the accuracy of covered data collected, processed, or transferred for a purpose described in subsection (b) and shall provide an effective mechanism for an individual to report inaccuracies in covered data.

(g) Data Minimization.—

(1) In General.—During the COVID–19 public health emergency, a covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall not collect, process, or transfer covered data beyond what is reasonably necessary, proportionate, and limited to carry out such purpose.
GUIDELINES.—Not later than 30 days after the date of enactment of this Act, the Commission shall issue guidelines recommending best practices for covered entities to minimize the collection, processing, and transfer of covered data in accordance with this subsection.

(h) PROTECTION OF COVERED DATA.—During the COVID–19 public health emergency, a covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risks to the confidentiality, security, and integrity of such data.

(i) EXCEPTION.—Notwithstanding subsection (a), a covered entity may collect, process, or transfer the covered data of an individual or group of individuals for a purpose described in subsection (b) during the COVID–19 public health emergency without obtaining the affirmative express consent of the individual if such collection, processing, or transfer is necessary to allow the covered entity to comply with a Federal, State, or local legal obligation.

SEC. 4. ENFORCEMENT.

(a) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act shall be treated as a violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—Except as provided in paragraph (4), the Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates such section shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act. Except as provided in subsection (c), enforcement by the Commission shall be the exclusive means of enforcing compliance with this Act.

(3) COOPERATION WITH OTHER AGENCIES.—Whenever the Commission obtains information that any covered entity may have processed or transferred covered data in violation of Federal anti-discrimination laws, the Commission shall transmit the information to the appropriate Federal or State agency with authority to initiate proceedings related to such violation.

(4) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS.—Notwithstanding section 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act in the same manner provided in paragraphs (1) and (2) of this subsection with respect to—

(A) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto; and

(B) organizations not organized to carry on business for their own profit or that of their members.

(b) EFFECT ON OTHER LAWS.—

(1) IN GENERAL.—Nothing in this Act shall be construed in any way to limit the authority of the Commission under any other provision of law.

(2) NONAPPLICATION OF FCC LAWS AND REGULATIONS TO COVERED ENTITIES.—Notwithstanding any other provision of law, neither any provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto nor any regulation promulgated by the Federal Communications Commission under such Acts shall apply to any covered entity with respect to the collection, processing, or transferring of covered data for a purpose described in section 3(b), except to the extent that such provision or regulation pertains solely to “911” lines or any other emergency line of a hospital, medical provider or service office, health care facility, poison control center, fire protection agency, or law enforcement agency.

(3) STATE PREEMPTION.—No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard to the extent that such law, regulation, rule, requirement, or standard is related to the collection, processing, or transfer of covered data for a purpose described in section 3(b).

(c) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) IN GENERAL.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by the engagement of any covered entity in an act or practice that violates this Act, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(A) enjoin that act or practice;

(B) enforce compliance with this Act or the regulation;
(C) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of the State; or
(D) obtain such other relief as the court may consider to be appropriate.

(2) RIGHTS OF THE COMMISSION.—

(A) IN GENERAL.—Except where not feasible, the attorney general of a State shall notify the Commission in writing prior to initiating a civil action under paragraph (1). Such notice shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notice, the Commission may intervene in such action and, upon intervening—

(i) be heard on all matters arising in such action; and
(ii) file petitions for appeal of a decision in such action.

(B) NOTIFICATION TIMELINE.—Where it is not feasible for the attorney general of a State to provide the notification required by subparagraph (A) before initiating a civil action under paragraph (1), the attorney general shall notify the Commission immediately after initiating the civil action.

(3) ACTIONS BY COMMISSION.—In any case in which a civil action is instituted by the Commission for violation of this Act, no attorney general of a State may, during the pendency of such action, institute a civil action against any defendant named in the complaint in the action instituted by the Commission for a violation of this Act that is alleged in such complaint.

(4) INVESTIGATORY POWERS.—Nothing in this Act shall be construed to prevent the attorney general of a State or another authorized official of a State from exercising the powers conferred on the attorney general or the State official by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(5) CONSOLIDATION OF ACTIONS BROUGHT BY TWO OR MORE STATE ATTORNEYS GENERAL OR AUTHORIZED STATE GOVERNMENTAL AUTHORITIES.—Whenever a civil action under paragraph (1) is pending and another civil action or actions are commenced pursuant to such paragraph in a different Federal district court or courts that involve 1 or more common questions of fact, such action or actions shall be transferred for the purposes of consolidated pretrial proceedings and trial to the United States District Court for the District of Columbia; provided however, that no such action shall be transferred if pretrial proceedings in that action have been concluded before a subsequent action is filed by a State attorney general or authorized State governmental authority.
116th CONGRESS
2d Session

S. 3749
To protect the privacy of health information during a national health emergency.

IN THE SENATE OF THE UNITED STATES
May 14, 2020

Mr. Blumenthal (for himself and Mr. Warner) introduced the following bill; which was read twice and referred to the Committee on Health, Education, Labor, and Pensions

A BILL

To protect the privacy of health information during a national health emergency.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.
This Act may be cited as the "Public Health Emergency Privacy Act".

SEC. 2. DEFINITIONS.
In this Act:
(1) Affirmative express consent.--The term "affirmative express consent" means an affirmative act by an individual that--
(A) clearly and conspicuously communicates the individual's authorization of an act or practice;
(B) is made in the absence of any mechanism in the
user interface that has the purpose or substantial effect of obscuring, subverting, or impairing decision making or choice to obtain consent; and

(C) cannot be inferred from inaction.

(2) Collect.--The term "collect", with respect to emergency health data, means obtaining in any manner by a covered organization.


(4) Covered organization.--

(A) In general.--The term "covered organization" means any person (including a government entity) --

(i) that collects, uses, or discloses emergency health data electronically or through communication by wire or radio; or

(ii) that develops or operates a website, web application, mobile application, mobile operating system feature, or smart device application for the purpose of tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the COVID-19 public health emergency.

(B) Exclusions.--The term "covered organization" does not include--

(i) a health care provider;

(ii) a person engaged in a de minimis collection or processing of emergency health data;

(iii) a service provider;

(iv) a person acting in their individual or household capacity; or

(v) a public health authority.

(5) Demographic data.--The term "demographic data" means information relating to the actual or perceived race, color, ethnicity, national origin, religion, sex, gender, gender identity, sexual orientation, age, Tribal affiliation, disability, domicile, employment status, familial status, immigration status, or veteran status of an individual or group of individuals.

(6) Device.--The term "device" means any electronic equipment that is primarily designed for or marketed to consumers.

(7) Disclosure.--The term "disclosure", with respect to emergency health data, means the releasing, transferring, selling, providing access to, licensing, or divulging in any manner by a covered organization to a third party.

(8) Emergency health data.--The term "emergency health data" means data linked or reasonably linkable to an individual or device, including data inferred or derived about the individual or device from other collected data provided such data is still linked or reasonably linkable to the individual or device, that concerns the public COVID-19 health emergency. Such data includes--

(A) information that reveals the past, present, or future physical or behavioral health or condition of, or provision of healthcare to, an individual, including--

(i) data derived from the testing or examination of a body part or bodily substance, or a request for such testing;

(ii) whether or not an individual has contracted or been tested for, or an estimate of the likelihood that a particular individual may contract, such disease or disorder; and

(iii) genetic data, biological samples, and biometrics; and

(B) other data collected in conjunction with other emergency health data or for the purpose of tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the COVID-19 public health emergency, including--

(i) geolocation data, when such term means data capable of determining the past or present precise physical location of an individual at a specific point in time, taking account of population densities, including cell-site location information, triangulation data derived from nearby wireless or radio frequency networks, and global positioning system data;

(ii) proximity data, when such term means information that identifies or estimates the past or present physical proximity of one
individual or device to another, including information derived from Bluetooth, audio signatures, nearby wireless networks, and near-field communications;
(iii) demographic data;
(iv) contact information for identifiable individuals or a history of the individual’s contacts over a period of time, such as an address book or call log; and
(v) any other data collected from a personal device.
(9) Government entity.--The term ‘government entity’ includes a Federal agency, a State, a local government, and other organizations, as such terms are defined in section 3371 of title 5, United States Code.
(10) Health care provider.--The term ‘health care provider’ has the meaning given the term ‘eligible health care provider’ in title VIII of division B of the CARES Act (Public Law 116–136).
(11) HIPAA regulations.--The term ‘HIPAA regulations’ means parts 160 and 164 of title 45, Code of Federal Regulations.
(12) Public health authority.--The term ‘public health authority’ means an entity that is authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, or disability including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions, and a person, such as a designated agency or associate, acting under a grant of authority from, or under a contract with, such public entity, including the employees or agents of such entity or its contractors or persons or entities to whom it has granted authority.
(13) COVID-19 public health emergency.--The term ‘COVID-19 public health emergency’ means the outbreak and public health response pertaining to Coronavirus Disease 2019 (COVID-19), associated with the emergency declared by the Secretary on January 31, 2020, under section 319 of the Public Health Service Act (42 U.S.C. 247d), and any renewals thereof and any subsequent declarations by the Secretary related to the coronavirus.
(14) Secretary.--The term ‘Secretary’ means the Secretary of Health and Human Services.
(15) Service provider.--
(A) In general.--The term ‘service provider’ means a person that collects, uses, or discloses emergency health data for the sole purpose of, and only to the extent that such entity is, conducting business activities on behalf of, for the benefit of, under instruction of, and under contractual agreement with a covered organization.
(B) Limitation of application.--Such person shall only be considered a service provider in the course of activities described in subparagraph (A).
(C) Exclusions.--The term ‘service provider’ excludes a person that develops or operates a website, web application, mobile application, or smart device application for the purpose of tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the COVID-19 public health emergency.
(16) State.--The term ‘State’ means each State of the United States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.
(17) Third party.--
(A) In general.--The term ‘third party’ means, with respect to a covered organization--
(i) another person to whom such covered organization disclosed emergency health data; and
(ii) a corporate affiliate or a related party of the covered organization that does not have a direct relationship with an individual with whom the emergency health data is linked or is reasonably linkable.
(B) Exclusion.--The term ‘third party’ excludes, with respect to a covered organization--
(i) a service provider of such covered organization; or
(ii) a public health authority.
Use.--The term "use", with respect to emergency health data, means the processing, employment, application, utilization, examination, or analysis of such data by a covered organization that maintains such data.

SEC. 3. PROTECTING THE PRIVACY AND SECURITY OF EMERGENCY HEALTH DATA.

(a) Right to Privacy.--A covered organization that collects emergency health data shall--

(1) only collect, use, or disclose such data that is necessary, proportionate, and limited for a good faith public health purpose, including a service or feature to support such a purpose;
(2) take reasonable measures, where possible, to ensure the accuracy of emergency health data and provide an effective mechanism for an individual to correct inaccurate information;
(3) adopt reasonable safeguards to prevent unlawful discrimination on the basis of emergency health data; and
(4) only disclose such data to a government entity when the disclosure--
(A) is to a public health authority; and
(B) is made in solely for good faith public health purposes and in direct response to exigent circumstances.

(b) Right to Security.--A covered organization or service provider that collects, uses, or discloses emergency health data shall establish and implement reasonable data security policies, practices, and procedures to protect the security and confidentiality of emergency health data.

(c) Prohibited Uses.--A covered organization shall not collect, use, or disclose emergency health data for any purpose not authorized under this section, including--

(1) commercial advertising, recommendation for e-commerce, or the training of machine-learning algorithms related to, or subsequently for use in, commercial advertising and e-commerce;
(2) soliciting, offering, selling, leasing, licensing, renting, advertising, marketing, or otherwise commercially contracting for employment, finance, credit, insurance, housing, or education opportunities in a manner that discriminates or otherwise makes opportunities unavailable on the basis of emergency health data; and
(3) segregating, discriminating in, or otherwise making unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation (as such term is defined in section 301 of the Americans With Disabilities Act of 1990 (42 U.S.C. 12181)), except as authorized by a State or Federal Government entity for a public health purpose notwithstanding subsection (g).

(d) Consent.--

(1) In general.--It shall be unlawful for a covered organization to collect, use, or disclose emergency health data, unless--
(A) the individual to whom the data pertains has given affirmative express consent to such collection, use, or disclosure;
(B) such collection, use, or disclosure is necessary and for the sole purpose of--
(i) protecting against malicious, deceptive, fraudulent, or illegal activity; or
(ii) detecting, responding to, or preventing information security incidents or threats; or
(C) the covered organization is compelled to do so by a legal obligation.

(2) Revocation.--

(A) In general.--A covered organization shall provide an effective mechanism for an individual to revoke consent after it is given.

(B) Effect.--After an individual revokes consent, the covered organization shall cease collecting, using, or disclosing the individual’s emergency health data as soon as practicable, but in no case later than 15 days after the receipt of the individual’s revocation of consent.

(C) Destruction.--Not later than 30 days after the receipt of an individual’s revocation of consent, a covered organization shall destroy or render not linkable that individual’s emergency health data under the same procedures in subsection (f).

(e) Notice.--A covered organization that collects, uses, or discloses emergency health data shall provide to an individual a privacy policy that--
(1) is disclosed in a clear and conspicuous manner, in the language in which the individual typically interacts with the covered organization, prior to or at the point of the collection of emergency health data;

(2) describes how and for what purposes the covered organization collects, uses, and discloses emergency health data, including the categories of recipients to whom it discloses data and the purpose of disclosure for each category;

(3) describes the covered organization's data retention and data security policies and practices for emergency health data; and

(4) describes how an individual may exercise the rights under this Act and how to contact the Commission to file a complaint.

(f) Public Reporting.--

(1) In general.--A covered organization that collects, uses, or discloses emergency health data of at least 100,000 individuals shall, at least once every 90 days, issue a public report--

(A) stating in aggregate terms the number of individuals whose emergency health data the covered organization collected, used, or disclosed to the extent practicable; and

(B) describing the categories of emergency health data collected, used, or disclosed, the purposes for which each such category of emergency health data was collected, used, or disclosed, and the categories of third parties to whom it was disclosed.

(2) Rules of construction.--Nothing in this subsection shall be construed to require a covered organization to--

(A) take an action that would convert data that is not emergency health data into emergency health data;

(B) collect or maintain emergency health data that the covered organization would otherwise not maintain; or

(C) maintain emergency health data longer than the covered organization would otherwise maintain such data.

(g) Required Data Destruction.--

(1) In general.--A covered organization may not use or maintain emergency health data of an individual after the later of--

(A) the date that is 60 days after the termination of the public health emergency declared by the Secretary on January 31, 2020, pertaining to Coronavirus Disease 2019 (COVID-19) under section 319 of the Public Health Service Act (42 U.S.C. 247d) and any renewals thereof;

(B) the date that is 60 days after the termination of a public health emergency declared by a governor or chief executive of a State pertaining to Coronavirus Disease 2019 (COVID-19) in which the individual resides; or

(C) 60 days after collection.

(2) Requirement.--For the requirements under paragraph (1), data shall be destroyed or rendered not linkable in such a manner that it is impossible or demonstrably impracticable to identify any individual from the data.

(3) Relation to certain requirements.--The provisions of this subsection shall not supersede any requirements or authorizations under--

(A) the Privacy Act of 1974 (Public Law 93-79);

(B) the HIPAA regulations; or

(C) Federal or State medical records retention and health privacy laws or regulations, or other applicable Federal or State laws.

(h) Emergency Data Collected, Used, or Disclosed Before Enactment.--

(1) Initiating a rulemaking.--Not later than 7 days after the date of enactment of this Act, the Commission shall initiate a public rulemaking to promulgate regulations to ensure a covered organization that has collected, used, or disclosed emergency health data before the date of enactment of this Act is in compliance with this Act, to the degree practicable.

(2) Completing a rulemaking.--The Commission shall complete the rulemaking within 45 days after the date of enactment of this Act.

(i) Non-Application to Manual Contact Tracing and Case Investigation.--Nothing in this Act shall be construed to limit or prohibit a public health authority from administering programs or activities to identify individuals who have contracted, or may have
been exposed to, COVID-19 through interviews, outreach, case investigation, and other recognized investigatory measures by a public health authority or their designated agent by a public health authority or their designated agent intended to monitor and mitigate the transmission of a disease or disorder.

(j) Research and Development.--This section shall not be construed to prohibit--

(1) public health or scientific research associated with the COVID-19 public health emergency by--

(A) a public health authority;

(B) a nonprofit organization, as described in section 501(c)(3) of the Internal Revenue Code of 1986; or

(C) an institution of higher education, as such term is defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001); or

(2) research, development, manufacture, or distribution of a drug, biological product, or vaccine that relates to a disease or disorder that is associated or potentially associated with a public health emergency.

(k) Legal Requirements.--Notwithstanding subsection (a)(5), nothing in this Act shall be construed to prohibit a good faith response to, or compliance with, otherwise valid subpoenas, court orders, or other legal processes, or to prohibit storage or providing information as otherwise required by law.

(l) Application to HIPAA Covered Entities.--

(1) In general.--This Act does not apply to a `covered entity' or a person acting as a `business associate' under the HIPAA regulations (to the extent that such entities or associates are acting in such capacity) or any health care provider.

(2) Guidance for consistency.--Not later than 30 days after the date of enactment of this Act, the Secretary shall promulgate guidance on the applicability of requirements, similar to those in this section to `covered entities' and persons acting as `business associates' under the HIPAA regulations. In promulgating such guidance, the Secretary shall reduce duplication of requirements and may exclude a requirement of this section if such requirement is already a requirement of the HIPAA regulations.

SEC. 4. PROTECTING THE RIGHT TO VOTE.

(a) In General.--A government entity may not, and a covered organization may not knowingly facilitate, on the basis of an individual's emergency health data, medical condition, or participation or non-participation in a program to collect emergency health data--

(1) deny, restrict, or interfere with the right to vote in a Federal, State, or local election;

(2) attempt to deny, restrict, or interfere with the right to vote in a Federal, State, or local election; or

(3) retaliate against an individual for voting in a Federal, State, or local election.

(b) Civil Action.--In the case of any violation of subsection (a), an individual may bring a civil action to obtain appropriate relief against a government entity in a Federal district court.

SEC. 5. REPORTS ON CIVIL RIGHTS IMPACTS.

(a) Report Required.--The Secretary, in consultation with the United States Commission on Civil Rights and the Commission, shall prepare and submit to Congress reports that examines the civil rights impact of the collection, use, and disclosure of health information in response to the COVID-19 public health emergency.

(b) Scope of Report.--Each report required under subsection (a) shall, at a minimum--

(1) evaluate the impact of such practices on civil rights and protections for individuals based on race, color, ethnicity, national origin, religion, sex, gender, gender identity, sexual orientation, age, Tribal affiliation, disability, domicile, employment status, familial status, immigration status, or veteran status;

(2) analyze the impact, risks, costs, legal considerations, disparate impacts, and other implications to civil rights of policies to incentivize or require the adoption of digital tools or apps used for contact tracing, exposure notification, or health monitoring; and

(3) include recommendations on preventing and addressing undue or disparate impact, segregation, discrimination, or infringements of civil rights in the collection and use of health information, including during a national health emergency.
(c) Timing...

(1) Initial report.--The Secretary shall submit an initial report under subsection (a) not sooner than 9 months, and not later than 12 months after the date of enactment of this Act.

(2) Subsequent reports.--The Secretary shall submit reports annually after the initial report required under paragraph (1) until 1 year after the termination of any public health emergency pertaining to Coronavirus Disease 2019 (COVID-19) under section 319 of the Public Health Service Act (42 U.S.C. 247d).

SEC. 6. ENFORCEMENT.

(a) Federal Trade Commission.--

(1) Unfair or deceptive acts or practices.--A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) Powers of commission.--The Commission shall enforce this Act and the regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act. Provided, however, that, notwithstanding the requirements of section 16(a) of the Federal Trade Commission Act (15 U.S.C. 56(a)), the Commission shall have the exclusive authority to commence or defend, and supervise the litigation of, any action for a violation of this Act or a regulation promulgated under this Act and any appeal of such action in its own name by any of its attorneys designated by it for such purpose, without first referring the matter to the Attorney General.

(3) Rulemaking authority.--

(A) In general.--The Commission shall have authority under section 553 of title 5, United States Code, to promulgate any regulations necessary to implement this Act.

(B) Consultation.--In promulgating any regulations under this Act, the Commission shall consult with the Secretary.

(4) Common carriers and nonprofit organizations.--Notwithstanding section 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44; 45(a)(2); 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act, in the same manner provided in paragraphs (1) and (2) of this paragraph, with respect to:

(A) common carriers subject to the Acts to regulate commerce, air carriers, and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.), except as provided in section 486(b) of such Act (7 U.S.C. 227(b)); and

(B) organizations not organized to carry on business for their own profit or that of their members.

(b) Enforcement by States.--

(1) In general.--In any case in which the attorney general of a State has reason to believe that an interest of the residents of the State has been or is threatened or adversely affected by the engagement of any person subject to this Act in a practice that violates such subsection, the attorney general of the State may, as parens patriae, bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to obtain appropriate relief.

(2) Rights of the federal trade commission.--

(A) Notice to federal trade commission.--

(i) In general.--Except as provided in clause (iii), the attorney general of a State shall notify the Commission in writing that the attorney general intends to bring a civil action under paragraph (1) before initiating the civil action against a person subject to this Act.

(ii) Contents.--The notification required by clause (i) with respect to a civil action shall include a copy of the complaint to be
filed to initiate the civil action.

(iii) Exception.--If it is not feasible for the attorney general of a State to provide the notification required by clause (i) before initiating a civil action under paragraph (1), the attorney general shall notify the Commission immediately upon instituting the civil action.

(B) Intervention by the federal trade commission.--

The Commission may--

(i) intervene in any civil action brought by the attorney general of a State under paragraph (1); and

(ii) upon intervening--

(I) be heard on all matters arising in the civil action; and

(II) file petitions for appeal of a decision in the civil action.

(C) Investigatory powers.--Nothing in this subsection may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(3) Action by the federal trade commission.--If the Commission institutes a civil action with respect to a violation of this Act, the attorney general of a State may not, during the pendency of such action, bring a civil action under paragraph (1) of this subsection against any defendant named in the complaint of the Commission for the violation with respect to which the Commission instituted such action.

(4) Venue; service of process.--

(A) Venue.--Any action brought under paragraph (1) may be brought in--

(i) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(ii) another court of competent jurisdiction.

(B) Service of process.--In an action brought under paragraph (1), process may be served in any district in which the defendant--

(i) is an inhabitant; or

(ii) may be found.

(C) Actions by other state officials.--

(i) In general.--In addition to civil actions brought by attorneys general under paragraph (1), any other officer of a State who is authorized by the State to do so may bring a civil action under paragraph (1), subject to the same requirements and limitations that apply under this subsection to civil actions brought by attorneys general.

(ii) Savings provision.--Nothing in this subsection may be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

(c) Private Right of Action.--

(1) Enforcement by individuals.--

(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 $100 and not greater than $1,000 per violation against any person who negligently violates a provision of this Act;

(ii) an amount not less than $500 and not greater than $5,000 per violation against any person who recklessly, willfully, 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.
(C) Injury in fact.--A violation of this Act with respect to the emergency health data of an individual constitutes a concrete and particularized injury in fact to that individual.

(2) Invalidity of pre-dispute arbitration agreements and pre-dispute joint action waivers.--

(A) In general.--Notwithstanding any other provision of law, no pre-dispute arbitration agreement or pre-dispute joint action waiver shall be valid or enforceable with respect to a dispute arising under this Act.

(B) Applicability.--Any determination as to whether or how this subsection applies to any dispute shall be made by a court, rather than an arbitrator, without regard to whether such agreement purports to delegate such determination to an arbitrator.

(C) Definitions.--In this subsection:

(i) The term pre-dispute arbitration agreement means any agreement to arbitrate a dispute that has not arisen at the time of making the agreement.

(ii) The term pre-dispute joint-action waiver means an agreement, whether or not part of a pre-dispute arbitration agreement, that would prohibit, or waive the right of, one of the parties to the agreement to participate in a joint, class, or collective action in a judicial, arbitral, administrative, or other forum, concerning a dispute that has not yet arisen at the time of making the agreement.

(iii) The term dispute means any claim related to an alleged violation of this Act and between an individual and a covered organization.

SEC. 7. NONPREEMPTION.

Nothing in this Act shall preempt or supersede, or be interpreted to preempt or supersede, any Federal or State law or regulation, or limit the authority of the Commission or the Secretary under any other provision of law.

SEC. 8. EFFECTIVE DATE.

(a) In General.--This Act shall apply beginning on the date that is 30 days after the date of enactment of this Act.

(b) Authority To Promulgate Regulations and Take Certain Other Actions.--Nothing in subsection (a) affects--

(1) the authority of any person to take an action expressly required by a provision of this Act before the effective date described in such subsection; or

(2) the authority of the Commission to promulgate regulations to implement this Act or begin a rulemaking to promulgate such regulations.

<all>
S. 3861 - Exposure Notification Privacy Act
116th Congress (2019-2020) | Get alerts

Sponsor: Sen. Cantwell, Maria [D-WA] (Introduced 06/01/2020)
Committees: Senate - Commerce, Science, and Transportation
Latest Action: Senate - 06/01/2020 Read twice and referred to the Committee on Commerce, Science, and Transportation. (All Actions)
Tracker: Introduced Passed Senate Passed House To President Became Law

There is one version of the bill.

Text available as: XML/HTML | XML/HTML (new window) | TXT | PDF (PDF provides a complete and accurate display of this text.) ?

Shown Here:
Introduced in Senate (06/01/2020)

116TH CONGRESS
2d SESSION

S. 3861

To establish privacy requirements for operators of infectious disease exposure notification services.

IN THE SENATE OF THE UNITED STATES
JUNE 1, 2020

Ms. CANTWELL (for herself and Mr. CASSIDY) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To establish privacy requirements for operators of infectious disease exposure notification services.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.—This Act may be cited as the “Exposure Notification Privacy Act”.

(b) Table of Contents.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
Sec. 3. Public trust in automated exposure notification services.
Sec. 4. Voluntary participation and transparency.
Sec. 5. Data restrictions.
Sec. 6. Data deletion.
Sec. 7. Data security.
Sec. 8. Freedom of movement and nondiscrimination.
Sec. 9. Oversight.
Sec. 10. Enforcement.

SEC. 2. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE EXPRESS CONSENT.—

(A) IN GENERAL.—The term “affirmative express consent” means an affirmative act by an individual that clearly communicates the individual’s authorization for an act or practice, in response to a specific request that—
(i) is provided to the individual in a clear and conspicuous disclosure that is separate from other options or acceptance of general terms; and
(ii) includes a description of each act or practice for which the individual’s consent is sought and—
   (I) is written concisely and in easy-to-understand language; and
   (II) includes a prominent heading that would enable a reasonable individual to identify and understand the act or practice.

(B) EXPRESS CONSENT REQUIRED.—Affirmative express consent shall not be inferred from the inaction of an individual or the individual’s continued use of a service or product.

(C) VOLUNTARY.—Affirmative express consent shall be freely given and nonconditioned.

(2) AGGREGATE DATA.—The term “aggregate data” means information that relates to a group or category of individuals that is not linked or reasonably linkable to any individual or device that is linked or reasonably linkable to an individual, provided that a platform operator or operator of an automated exposure notification service—
   (A) takes reasonable measures to safeguard the data from reidentification;
   (B) publicly commits in a conspicuous manner not to attempt to reidentify or associate the data with any individual or device linked or reasonably linkable to an individual;
   (C) processes the data for public health purposes only; and
   (D) contractually requires the same commitment for all transfers of the data.

(3) AUTHORIZED DIAGNOSIS.—The term “authorized diagnosis” means an actual, potential, or presumptive positive diagnosis of an infectious disease confirmed by a public health authority or a licensed health care provider.

(4) AUTOMATED EXPOSURE NOTIFICATION SERVICE.—
   (A) IN GENERAL.—The term “automated exposure notification service” means a website, online service, online application, mobile application, or mobile operating system that is offered in commerce in the United States and that is designed, in part or in full, specifically to be used for, or marketed for, the purpose of digitally notifying, in an automated manner, an individual who may have become exposed to an infectious disease (or the device of such individual, or a person or entity that reviews such disclosures).
   (B) LIMITATIONS.—Such term does not include—
      (i) any technology that a public health authority uses as a means to facilitate traditional in-person, email, or telephonic contact tracing activities, or any similar technology that is used to assist individuals to evaluate if they are experiencing symptoms related to an infectious disease to the extent the technology is not used as an automated exposure notification service; or
      (ii) any platform operator or service provider that provides technology to facilitate an automated exposure notification service to the extent the technology acts only to facilitate such services and is not itself used as an automated exposure notification service.

(5) COLLECT; COLLECTION.—The terms “collect” and “collection” mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means, including by passively or actively observing the behavior of an individual.

(6) COVERED DATA.—The term “covered data” means any information that is—
   (A) linked or reasonably linkable to any individual or device linked or reasonably linkable to an individual;
   (B) not aggregate data; and
   (C) collected, processed, or transferred in connection with an automated exposure notification service.

(7) DECEPTIVE ACT OR PRACTICE.—The term “deceptive act or practice” means a deceptive act or practice in violation of section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)).

(8) DELETE.—The term “delete” means destroying, permanently erasing, or otherwise modifying covered data to make such covered data permanently unreadable or indecipherable and unrecoverable.

(9) EXECUTIVE AGENCY.—The term “Executive agency” has the meaning given such term in section 105 of title 5, United States Code.

(10) INDIAN TRIBE.—The term “Indian tribe”—
   (A) has the meaning given such term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304); and
   (B) includes a Native Hawaiian organization as defined in section 6207 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7517).
(11) OPERATOR OF AN AUTOMATED EXPOSURE NOTIFICATION SERVICE.—The term “operator of an automated exposure notification service” means any person or entity that operates an automated exposure notification service, other than a public health authority, and that is—

(A) subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.); or

(B) described in section 10(a)(4).

(12) PLATFORM OPERATOR.—The term “platform operator” means any person or entity other than a service provider who provides an operating system that includes features supportive of an automated exposure notification service and facilitates the use or distribution of such automated exposure notification service to the extent the technology is not used by the platform operator as an automated exposure notification service.

(13) PROCESS.—The term “process” means any operation or set of operations performed on covered data, including collection, analysis, organization, structuring, retaining, using, securing, or otherwise handling covered data.

(14) PUBLIC HEALTH AUTHORITY.—The term “public health authority” means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe that is responsible for public health matters as part of its official mandate, or a person or entity acting under a grant of authority from or contract with such public agency.

(15) SERVICE PROVIDER.—The term “service provider” means any person or entity, other than a platform operator, that processes or transfers covered data in the course of performing a service or function on behalf of, and at the direction of, a platform operator, an operator of an automated exposure notification service, or a public health authority, but only to the extent that such processing or transfer relates to the performance of such service or function.

(16) STATE.—The term “State” means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

(17) TRANSFER.—The term “transfer” means to disclose, release, share, disseminate, make available, allow access to, sell, license, or otherwise communicate covered data by any means to a nonaffiliated entity or person.

SEC. 3. PUBLIC TRUST IN AUTOMATED EXPOSURE NOTIFICATION SERVICES.

(a) COLLABORATION WITH PUBLIC HEALTH.—An operator of an automated exposure notification service shall collaborate with a public health authority in the operation of such service.

(b) DIAGNOSIS INFORMATION.—An operator of an automated exposure notification service may not collect, process, or transfer an actual, potential, or presumptive positive diagnosis of an infectious disease as part of the automated exposure notification service, unless such diagnosis is an authorized diagnosis.

(c) ACCURACY AND RELIABILITY.—An operator of an automated exposure notification service shall publish—

(1) guidance for the public on the functionality of the service and how to interpret the notifications, including any limitation with respect to the accuracy or reliability of the exposure risk; and

(2) measures of the effectiveness of the service offered, including adoption rates.

(d) PREVENTION OF DECEPTIVE ACTS OR PRACTICES.—It shall be unlawful for a platform operator or an operator of an automated exposure notification service to engage in a deceptive act or practice concerning an automated exposure notification service.

(e) SERVICE PROVIDER REQUIREMENT.—When a service provider has actual knowledge that an operator of an automated exposure notification service or a public health authority has engaged in an act or practice that fails to adhere to the standards set forth in sections 3 through 8 of this Act, the service provider shall notify the automated exposure notification service or the public health authority, as applicable, of the potential violation or failure to adhere to such standards.

SEC. 4. VOLUNTARY PARTICIPATION AND TRANSPARENCY.

(a) VOLUNTARY PARTICIPATION.—

(1) ENROLLMENT WITH AFFIRMATIVE EXPRESS CONSENT.—An operator of an automated exposure notification service—

(A) may not enroll an individual in the automated exposure notification service without the individual’s prior affirmative express consent; and

(B) shall provide an individual with a clear and conspicuous means to withdraw affirmative express consent to the individual’s enrollment in the automated exposure notification service.

(2) RIGHT TO IDENTIFY A DIAGNOSIS.—An individual with an authorized diagnosis shall determine whether the individual’s authorized diagnosis is processed as part of the automated exposure notification service.

(b) NOTICE OF COVERED DATA PRACTICES.—An operator of an automated exposure notification service and a platform operator shall make publicly and persistently available, in a conspicuous and readily accessible manner, a privacy policy that provides a detailed and accurate representation of that person or entity’s covered data collection, processing, and
transfer activities in connection with such person or entity’s automated exposure notification service or the facilitation of such service. Such privacy policy shall include, at a minimum—

1. the identity and the contact information of the person or entity, including the contact information for the person or entity’s representative for privacy and covered data security inquiries;

2. each category of covered data the person or entity collects and the limited allowable processing purposes for which such covered data is collected in accordance with section 5;

3. whether the person or entity transfers covered data for the limited allowable purposes in section 5 and, if so, a detailed description of the data transferred, the purpose of the transfer, and the identity of the recipient of the transfer;

4. a description of the person or entity’s covered data minimization and retention policies;

5. how an individual can exercise the individual rights described in this title;

6. a description of the person or entity’s covered data security policies; and

7. the effective date of the privacy policy.

(c) Languages.—A person or entity shall make the privacy policy required under this section available to the public in all of the languages in which the person or entity provides, or facilitates the provision of, an automated exposure notification service.

SEC. 5. DATA RESTRICTIONS.

(a) Collection and Processing Restrictions.—An operator of an automated exposure notification service may not collect or process any covered data—

1. beyond the minimum amount necessary to implement an automated exposure notification service for public health purposes; or

2. for any commercial purpose.

(b) Transfer Restrictions.—An operator of an automated exposure notification service may not transfer any covered data, except—

1. to provide notification of a potential exposure to an individual who has enrolled in the automated exposure notification service;

2. to a public health authority for public health purposes related to an infectious disease;

3. to its service provider, by contract, to—

   (A) perform system maintenance, debug systems, or repair any error to ensure the functionality of the automated exposure notification service, provided such processing is limited to this purpose; or

   (B) detect or respond to a security incident, provide a secure environment, or maintain the safety of the automated exposure notification service, provided such process is limited to this purpose; or

4. to comply with the establishment, exercise, or defense of a legal claim.

(c) Further Restrictions.—

1. In General.—It shall be unlawful for any person, entity, or Executive agency to transfer covered data to any Executive agency unless the information is transferred in connection with an investigation or enforcement proceeding under this Act.

2. Prohibition.—An Executive agency may not process or transfer covered data, except—

   (A) for a public health purpose related to an infectious disease; or

   (B) in connection with an investigation or enforcement proceeding under this Act.

(d) Research.—This section shall not be construed to prohibit data collection, processing, or transfers to carry out research—

1. conducted pursuant to the Federal policy for the protection of human subjects under part 46 of title 45, Code of Federal Regulations; or

2. for the development, manufacture, or distribution of a drug, biological product, or vaccine that relates to an infectious disease conducted pursuant to part 50 of title 21, Code of Federal Regulations.

SEC. 6. DATA DELETION.

(a) Deletion Upon Request.—Upon the request of an individual, an operator of an automated exposure notification service shall delete, or allow the individual to delete, all covered data of the individual that is processed by the operator.

(b) Recurring Deletion.—An operator of an automated exposure notification service shall delete the covered data of a participating individual within 30 days of receipt of such covered data, on a rolling basis, or at such times as is consistent with a standard published by a public health authority within an applicable jurisdiction.
(c) **Applicability To Service Providers.**—An operator of an automated exposure notification service shall instruct any service provider to which the entity transfers covered data to delete such data in accordance with the requirements of this subsection.

(d) **Research.**—This section shall not be construed to prohibit data retention for public health research purposes consistent with the requirements in section 5(d).

**SEC. 7. DATA SECURITY.**

(a) **In General.**—An operator of an automated exposure notification service shall establish, implement, and maintain data security practices to protect the confidentiality, integrity, availability, and accessibility of covered data. Such covered data security practices shall be consistent with standards generally accepted by experts in the information security field.

(b) **Specific Requirements.**—Covered data security practices required under subsection (a) shall include, at a minimum, the following:

1. **Assess Risks and Vulnerabilities.**—Identifying and assessing any reasonably foreseeable risks to, and vulnerabilities in, each system maintained by the person or entity that processes or transfers covered data, including unauthorized access to or risks to covered data, human and technical vulnerabilities, access rights, and use of service providers. Such activities shall include a plan to receive and respond to unsolicited reports of risks and vulnerabilities by entities and individuals, developing and testing systems for monitoring the security of covered data, and resilience against denial of service attacks and malicious disinformation.

2. **Preventive and Corrective Action.**—Taking preventive and corrective action to mitigate any risks or vulnerabilities to covered data identified by the person or entity, which may include implementing administrative, technical, or physical safeguards or changes to covered data security practices or the architecture, installation, or implementation of network or operating software.

3. **Breach Notification.**—Maintaining plans for responding to security incidents involving covered data and, in the most expedient time possible, consistent with the legitimate needs of law enforcement, notifying any individual whose data is subject to a security breach, as well as the Federal Trade Commission, of the breach, the data involved, any reasonably foreseeable impacts of the breach for individuals whose data is subject to the breach, the steps individuals may take to mitigate those impacts, and the measures the operator of the automated exposure notification service is taking to prevent a future incident. An operator of an automated exposure notification service shall require its service providers to provide notice to the operator of the automated exposure notification service of any breach of the security of the covered data immediately following the discovery of the breach.

(c) **Interference Prohibited.**—It shall be unlawful for any person or entity to transmit signals with the intent to cause an automated exposure notification service to produce inaccurate notifications or to otherwise interfere with the intended functioning of such a service.

**SEC. 8. FREEDOM OF MOVEMENT AND NONDISCRIMINATION.**

It shall be unlawful for any person or entity to segregate, discriminate against, or otherwise make unavailable to an individual or class of individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation (as such term is defined in section 301 of the Americans With Disabilities Act of 1990 (42 U.S.C. 12181)), based on covered data collected or processed through an automated exposure notification service or an individual's choice to use or not use an automated exposure notification service.

**SEC. 9. OVERSIGHT.**

(a) **In General.**—Section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee) is amended—

1. in subsection (c)—

   (A) in paragraph (1), by inserting “or to respond to health-related epidemics” after “from terrorism”; and

   (B) in paragraph (2), by inserting “or to respond to health-related epidemics” after “against terrorism”; and

2. in subsection (d)—

   (A) in paragraph (1), by inserting “or to respond to health-related epidemics” after “from terrorism” each place it appears; and

   (B) in paragraph (2)—

      (i) in subparagraph (B), by striking “and” at the end;

      (ii) in subparagraph (C), by striking the period at the end and inserting “; and”; and

      (iii) by adding at the end the following:

      “(D) the collection, use, storage, and sharing of covered data by Federal, State, or local government in connection with responding to a Federal declaration of a public health emergency to ensure that privacy and civil liberties are protected.”.
Section 10. Enforcement.

(a) Enforcement by the Federal Trade Commission.—

(1) Unfair or Deceptive Acts or Practices.—A violation of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(g)(1)(B)).

(2) Powers of the Commission.—

(A) In General.—Except as provided in paragraphs (3) and (4) of this subsection, the Federal Trade Commission (referred to in this Act as the “Commission”) shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(B) Privileges and Immunities.—Any person who violates this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(C) Effect on Other Laws.—Nothing in this Act shall be construed to limit the authority of the Commission under any other provision of law.

(3) Independent Litigation Authority.—Notwithstanding section 16 of the Federal Trade Commission Act (15 U.S.C. 56), the Commission may commence, defend, or intervene in, and supervise the litigation of, any civil action under this Act (including an action to collect a civil penalty) and any appeal of such action in its own name by any of its attorneys designated by it for such purpose. The Commission shall notify the Attorney General of any such action and may consult with the Attorney General with respect to any such action or request the Attorney General on behalf of the Commission to commence, defend, or intervene in any such action.

(4) Nonprofit Organizations and Communications Common Carriers.—Notwithstanding section 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any other jurisdictional limitation of the Commission, the Commission shall also enforce this Act in the same manner provided in paragraphs (1), (2), and (3) of this subsection, with respect to—

(A) any organization not organized to carry on business for the organization’s own profit or that of the organization’s members; and

(B) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto.

(b) Enforcement by State Attorneys General.—

(1) In General.—If the chief law enforcement officer of a State, or an official or agency designated by a State, has reason to believe that any person has violated or is violating this Act, the attorney general, official, or agency of the State, in addition to any authority it may have to bring an action in State court under its consumer protection law, may bring a civil action in any appropriate United States district court or in any other court of competent jurisdiction, including a State court, to—

(A) enjoin further such violation by such person;

(B) enforce compliance with this Act;

(C) obtain civil penalties; and

(D) obtain damages, restitution, or other compensation on behalf of residents of the State.

(2) Notice and Intervention by the FTC.—The attorney general of a State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of the complaint in
the action, except in any case in which such prior notice is not feasible, in which case the attorney general shall serve such notice immediately upon instituting such action. The Commission shall have the right—

(A) to intervene in the action;
(B) upon so intervening, to be heard on all matters arising therein; and
(C) to file petitions for appeal.

(3) RELATIONSHIP WITH STATE LAW CLAIMS.—If the attorney general of a State has authority to bring an action under State law directed at any act or practice that also violates this Act, the attorney general may assert the State law claim and a claim under this Act in the same civil action.

(c) STATE LAW PRESERVATION.—Nothing in this Act shall be construed to preempt, displace, or supplant any State law, rule, regulation, or requirement, including—

(1) any consumer protection law of general applicability such as any law regulating deceptive, unfair, or unconscionable practices;
(2) any health privacy or infectious disease law;
(3) any civil rights law;
(4) any law that governs the privacy rights or other protections of employees, employee information, or students or student information;
(5) any law that addresses notification requirements in the event of a covered data breach;
(6) contract or tort law;
(7) any criminal law governing fraud, theft, unauthorized access to information or unauthorized use of information, malicious behavior, and similar provisions, and any law of criminal procedure;
(8) any law specifying a remedy or a cause of action to an individual; or
(9) any public safety or sector-specific law unrelated to privacy or security.

(d) PRESERVATION OF COMMON LAW OR STATUTORY CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this Act, nor any amendment, standard, rule, requirement, assessment, law, or regulation promulgated under this Act, shall be construed to preempt, displace, or supplant any Federal or State common law right or remedy, or any statute creating a remedy for civil relief, including any cause of action for personal injury, wrongful death, property damage, or other financial, physical, reputational, or psychological injury based in negligence, strict liability, products liability, failure to warn, an objectively offensive intrusion into the private affairs or concerns of the individual, or any other legal theory of liability under any Federal or State common law, or any State statutory law.

(e) SEVERABILITY.—If any provision of this Act, or the application thereof to any person or entity or circumstance, is held invalid, the remainder of this Act and the application of such provision to other persons or entities not similarly situated or to other circumstances shall not be affected by the invalidation.

(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are necessary to carry out this Act and the amendments made by this Act.

(g) EFFECTIVE DATE.—This Act and the amendments made by this Act shall take effect on the date of the enactment of this Act.