Published on *The National Law Review* https://natlawreview.com

COVID-19 Privacy Implications: Workplace Temperature Screening

Article By:

Jeffrey M. Stefan II

While preparing to reopen offices, companies are assessing various screening programs to mitigate the risk of spreading COVID-19. Symptom and temperature screening has been endorsed by the White House[1] and Centers for Disease Control and Prevention (CDC)[2], as well as the Equal Employment Opportunity Commission (EEOC).[3] Some states even require employers to conduct regular temperature checks on employees. For example, Colorado requires certain critical and non-critical businesses to conduct daily temperature checks and monitor employees' symptoms, and employers with 50 or more employees at one location must implement stations for symptom screenings and temperature checks.[4]

Temperature screening can be conducted in a number of ways. Employers could require employees to take their own temperatures at home, designate one or more employees to manually conduct the screenings on-site or employ an automated no-contact screening method. A number of technologies are available for no-contact temperature screening, such as infrared scanners (raygun-like devices aimed at a person's forehead which estimates the body's internal temperature), facial recognition and thermal scanning devices, and wearables like watches and stick-on sensors which can often be paired with smartphone apps.

While these devices are a convenient way to monitor employees for fevers and mitigate the spread of COVID-19 in the workplace, companies should be mindful that collecting information through temperature screening devices could come with heightened privacy obligations due to the potential sensitivity of the information.

To mitigate privacy and security compliance risks, the following is recommended when considering whether and how to implement a temperature screening program:

Understand privacy implications when determining the best screening approach.

Reducing the amount of sensitive information your company collects will reduce the risk of a data breach or other privacy law violations. This is true both domestically and internationally, depending on where employees are based. **If your company opts to implement a temperature screening policy, some of the obligations that may be triggered include:**

- **State Data Breach Laws:** Every state in the U.S. has enacted a data breach notification statute which, depending on the nature of the breach, could require a company to notify individuals, State Attorneys General, and federal credit reporting and investigative agencies. Some of the laws require an offer of credit monitoring services.
- The more sensitive the data, the higher likelihood that these state statutes and related obligations will be triggered. Several state data breach statutes and privacy laws[5] require personally identifiable medical information be secured from unauthorized access or breach. This would include an employee's first name or first initial and last name in combination with medical information (e.g., results from temperature tests, information about the employee's taste/smell, testing for the virus, doctors' notes or similar information).
- **The FTC Act and CCPA:** If you implement a temperature screening program, the FTC Act and CCPA (for California residents) require that your privacy statements (and other disclosures) are transparent about the personal information that is collected as part of the screening and how it is used and shared. CCPA may also give an employee the right to request access or deletion of the information, subject to applicable exceptions.
- **Americans With Disabilities Act (ADA)**: The ADA prohibits an employer from making disability-related inquiries and requiring medical examinations of employees, except under limited circumstances. While the EEOC has recently clarified that employers may implement temperature checks and make inquiries about COVID-19 symptoms, broader monitoring activities and inquiries about symptoms **not** directly related to COVID-19 are still subject to the ADA requirements.[6] The ADA also has strict regulations regarding disclosure of the identity of an employee who has tested positive for COVID-19.
- **Global Data Protection Regulation (GDPR):** GDPR applies to all companies processing the personal data of European Union residents. This information, even if it just notes that a temperature is "high" or "within a normal range," will constitute "data concerning health" under the GDPR. By recording this data, you will be processing a "special category of personal data." The GDPR generally prohibits processing of this kind of data unless you can demonstrate you satisfy certain enumerated legal grounds.[7]
- **Health Information Portability and Accountability Act (HIPAA):** HIPAA should **not** trigger additional obligations on employers that conduct temperature screening because an employer's HIPAA obligations are generally limited only to covered health plans that are sponsored by the business.

If temperature screening is conducted using cameras and facial-recognition technology, make sure the necessary disclosures have been made and the proper consents are obtained.

Body temperature alone is not biometric information; however, face scans and fingerprints are. There are a number of state laws which require businesses to provide adequate notice and, at times, obtain affirmative consent before collecting biometric information from individuals. The most notable of these are the California Consumer Privacy Act (CCPA) and the Illinois Biometric Privacy Act (BIPA).

- **Companies doing business in California need to give proper notice:** Companies that do business in California and have in excess of $25 million in annual gross revenues or otherwise process or sell large amounts of personal information of California residents have certain specific obligations to consider. Under the CCPA, beginning in January 2021 employers must provide employees with CCPA-compliant privacy disclosures anytime they collect certain personal information, including medical information, facial scans and most of the information collected using smartphone apps. The notice must explain what information

will be collected and the purpose/use of such collection. The information collected may not be used for any purpose other than what is disclosed in the notice. Intentional violations of the CCPA may result in civil penalties of up to $7,500 for each violation.

- **Companies collecting the biometric information of Illinois residents need to give proper notice AND obtain written consent from individuals:** The BIPA requires private entities that collect, retain or disclose biometric information to follow certain requirements to ensure that individuals have consented to such data collection. Those entities must develop publicly-available written policies which detail retention schedules and guidelines for permanent deletion of the information once the purpose of collecting the information is satisfied. There have been dozens of BIPA-related lawsuits against employers in recent months, and individuals are entitled to the greater of actual or liquidated damages of up to $1,000 for each negligent violation of the BIPA or $5,000 for each intentional or reckless violation of the BIPA.
- Though Illinois is the only state that has a private right of action for violations of its biometric privacy law, Texas and Washington have enacted similar laws which allow their attorneys general to bring enforcement actions against violators.

Thoroughly vet any third party who is assisting with screening or whose software is being used for screening employees.

If your company is using the services of a third party to screen employees (i.e., for elevated temperatures), including mobile applications developed by third parties, it is important to review these agreements and make sure that they include sufficient privacy and security provisions that address their obligations and limited use rights as it relates to the personal information being collected through the screening.

Adequately protect the information collected from employees and maintain the confidentiality of that information.

Whether the information from temperature screenings is collected by employees at home or collected on-site, it must be adequately protected and kept confidential. Collected information should be shared only with those who have a need to know and should be protected under HIPAA standards. Employers must also maintain all information about an employee's illness as a confidential medical record in compliance with the ADA, separate from the employee's personnel file.

Many states also have laws requiring businesses to maintain adequate safeguards to protect personal information. For example, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) requires businesses to implement and maintain information security protocols, and its definition of personal information was recently amended to include biometric information.

[1] https://www.whitehouse.gov/openingamerica

[2] https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html; https://www.cdc.gov/coronavirus/2019-ncov/downloads/community-mitigation-strategy.pdf

[3] https://www.eeoc.gov/wysk/what-you-should-know-about-ada-rehabilitation-act-and-coronavirus

[4] https://drive.google.com/file/d/107dLRAJaD4ZtNJGy8geSf0UvngesvKYd/view

[5] *See, e.g.*, Ala. Code § 8-38-2(6); 815 ILCS 530/5.; § 407.1500(1)(9), RSMo; 2019 Wash. Sess. Laws Ch. 241. S.H.B. 1071, § 1 (effective 3/1/20).

[6] https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act

[7] https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/workplace-testing-guidance-for-employers/

National Law Review, Volume X, Number 167

Source URL:https://natlawreview.com/article/covid-19-privacy-implications-workplace-temperature-screening