Bender's Labor & Employment Bulletin

October 2020
VOLUME 20 • ISSUE NO. 10

Inside This Issue

LexisNexis®
Matthew Bender®

Navigating Symptom Checker Applications, Privacy Concerns, and Workplace Discrimination; Considerations for Best Practices

By RyAnn McKay Hooper, Karen Mandelbaum, Steven M. Swirsky, Epstein Becker & Green P.C.

As many employers in the United States face the ever-looming question of when and how to return employees back to the physical workplace, and states and localities continue to develop and refine guidelines to offer guidance on "safe" return to in-person work, the development of digital tools to help manage the spread of COVID-19 have grown exponentially. In some places, employers are required by state law to screen the health of employees prior to reopening their business, and regularly thereafter to keep the business doors open. Mobile applications that track symptoms, or technology platforms that use detailed algorithms to allow users to input symptoms and receive diagnostic information, are becoming widely accepted as a tool business may use to reopen the workplace with reduced risk of COVID-19 transmission from employee-to-employee.

Digital tools which track and check health symptoms, provide employees with access to telehealth services, and provide employers with access to contact tracing capabilities are valuable tools in maintaining a virus-free or virus-light workplace. While there is no single body of law that protects employee personal data or that precludes an employer from requiring that employees returning to in person work utilize such applications, the use (or misuse) of the data collected by employers through these technologies and applications may leave an employer vulnerable to liability for issues related to consumer protection and data privacy, potential wage and hour issues, general discrimination, and general liability for third-party misuse of information collected. This article will explore the considerations and risks for employers evaluating the use of digital technologies and applications pursuant to local mandates requiring health screening for return-to-work.

COVID-19 Applications, Privacy and Security

COVID-19 Symptom Checker Applications ("apps") are designed to help protect the safety of employees returning to the workplace as well as to encourage customers, consumers, and employees to return to businesses by giving the staff and customers a sense that management is taking appropriate precautions to keep them safe and the relevant facilities as infection-free as possible. Applications come in various forms and offer a variety of functionalities. For example, some applications ask users to self-report symptoms

continued on page 247

CONTENTS:

ATTENTION READERS

Any reader interested in sharing information of interest to the labor and employment bar, including notices of upcoming seminars or newsworthy events, should direct this information to:

Laurie E. Leader
Law Offices of Laurie E. Leader, LLC
14047 W Petronella Dr., Suite 202B
Libertyville, IL 60048
E-mail: lleader51@gmail.com
or
Mary Anne Lenihan
Legal Editor
Bender's Labor & Employment Bulletin
LexisNexis Matthew Bender
230 Park Avenue, 7th Floor
New York, NY 10169
E-mail: maryanne.lenihan@lexisnexis.com

If you are interested in writing for the BULLETIN, please contact Laurie E. Leader via e-mail at lleader51@gmail.com or Mary Anne Lenihan via e-mail at maryanne.lenihan@lexisnexis.com.

A NOTE ON CITATION

The correct citation form for this publication is:
20 Bender's Lab. & Empl. Bull. 245 (October 2020)

ISBN 978-0-8205-5039-8, EBOOK ISBN 978-1-4224-8015-1

(Pub. 1239)

Navigating Symptom Checker Applications, Privacy Concerns, and Workplace Discrimination; Considerations for Best Practices
By RyAnn McKay Hooper, Karen Mandelbaum, Steven M. Swirsky, Epstein Becker & Green P.C.

(text continued from page 245)

and exposure to COVID-19, while others may perform a thermal scan of employee temperature or breathing pattern as they arrive to work and store the employee's temperature and respiratory rate information. More advanced and recently created applications permit companies to create online employee health surveys and map the workplace locations visited by employees to help trace the contacts of those who may develop coronavirus infections[1] or provide a daily symptom screener to help clear employees to go to work or direct them to be tested if they are at risk for infection.[2] In all of the above-scenarios, private and personal health information is actively collected from employees on a daily basis. In addition, the app user is often required to download the application on their own personal cell phone or device. This opens the door for the app developer to passively gather a multitude of additional information about the individual based on their web behavior and the way that a user has their preferences and permissions set for data sharing on their personal device.

An employee returning to work who is asked to provide certain information about their general health and potential for exposure to the coronavirus will have an interest in knowing that their data will be protected and remain confidential; however, when it comes to these apps, complete confidentiality and data protection are not currently accounted for under the law. A recent report conducted by the International Data Accountability Council (IDAC) analyzing more than one-hundred apps available to Android devices highlighted three main issues with privacy and the COVID-19 applications. First, the applications may utilize software development kits ("SDKs") maintained by third parties. The presence of an SDK allows for the potential transmission of private information for use or sale by a third party. Second, in the case of some apps, the data may be sent to the third-party in an unencrypted manner leaving the information vulnerable to hacking.[3] Third, the report concluded that in some cases, the surveyed applications were not always transparent about what information was collected, requested invasive permissions such as the location of the user or use of their personal device camera, and generally fell short of best practices for data collection.[4]

These issues highlight how important it is for businesses to thoroughly vet any application it is considering utilizing to help screen employees for return to work. Businesses should carefully consider whether the Terms and Conditions and the app's Privacy Policy offer adequate protection for the information their employees will have to provide. The Terms and Conditions and Privacy Policy form the legally binding agreement between the employer, as purchaser or licensee of the app, and the app developer and should include information about the underpinnings of its code or use of SDKs as well as what data is collected from users, how it will be used/disclosed and about what permissions the employee is agreeing to set their phone or device to in order to enable the technology.

Depending on the permissions of the application, the data collected may potentially go beyond data about basic temperature and exposure to the virus. The application may in some cases also collect protected demographic information – residence location or the location where the user most often accesses the app, age, race, gender, pre-existing conditions, weight, living conditions which heighten potential exposure (multi-generational living, homelessness, and other statuses) – all information that when used inappropriately can lend to claims of disparate treatment of the workforce.

EEOC Guidelines, Health Screening, and Return to Work

Because of the emergency and unprecedented nature of the pandemic, government entities have relaxed enforcement rules to some extent. Notably, the Equal Employment Opportunity Commission ("EEOC"), which enforces antidiscrimination rules that generally prohibits employers from requiring employees to undergo medical exams, said in March that, given the coronavirus threat, employers may

[1] Singer, Natasha. (11 May 2020). Employers Rush to Adopt Virus Screening. The Tools May Not Help Much. Retrieved from https://www.nytimes.com/2020/05/11/technology/coronavirus-worker-testing-privacy.html. Accessed September 12, 2020.

[2] Coombs, Bertha. (15 May 2020). Microsoft and UnitedHealth offer Companies Free App to Screen Employees for Coronavirus. Retrieved from https://www.cnbc.com/2020/05/15/microsoft-and-unitedhealth-offer-companies-free-app-to-screen-employees-for-coronavirus.html. Accessed September 12, 2020.

[3] Reuter, Elise. (8 June 2020). Report: Covid-19 Apps Fall Short in Privacy, Security. Retrieved from https://medcitynews.com/2020/06/report-many-covid-19-apps-fall-short-in-privacy-security/?rf=1. Accessed September 12, 2020.

[4] *Id.*

measure employees' temperatures.[5] More recently, the EEOC determined that COVID-19 tests, general symptom monitoring, and requiring medical certifications during the pandemic are not improper medical tools under the Americans with Disabilities Act ("ADA"), because they are job related and consistent with business necessity to protect employees in the workplace.[6] The new guidance stops short of permitting employers to require that employees submit to anti-body testing before returning to work, noting the EEOC's view that this would violate the ADA.

The EEOC has granted businesses permission to collect COVID-19 related health information of employees; however, it is important to remember that equal employment opportunity ("EEO") laws still apply during the pandemic and, therefore, how the data collected is used remains important. The EEOC guidelines rely heavily on principles established by the Center for Disease Control ("CDC"). According to the CDC, an employee who tests positive for COVID-19 is not eligible to return to the workforce in person, and therefore an employer may withdraw a job offer from that employee or withhold work.[7] A slight change in fact pattern, however, may yield a different result under EEO law. For example, if the prospective worker or worker tested negative for COVID-19, and the employer sought to inquire if the prospective worker lived with an individual who tested positive, this may result in an EEO violation. Employers should keep in mind that they may not discriminate against employees based on family status, and the employee's response to this inquiry could yield information that would not typically be relevant during the hiring process.[8] As with other screening measures, any inquiry regarding COVID-19 status or symptoms should be only be made after a conditional job offer has been made and such inquiries should be made consistently to all those being offered the position in question. Where questions are not uniformly asked of all employees or perspective employees, a business may also expose itself to liability for disparate treatment and discrimination.

Finally, employers must be mindful of how they collect and utilize data which may shows trends in COVID-19s impact on certain populations. The CDC has determined that long-standing systemic health and social inequities have put many people from racial and ethnic minority groups at increased risk of contracting COVID-19 as well as having higher mortality levels.[9] Further, the World Health Organization has determined that COVID-19 is often more severe in people who are older than 60 years or who have underlying health conditions such as lung or heart disease, diabetes and conditions that affect their immune systems.[10] Within that high risk population, autoimmune diseases affect approximately 8% of the population, 78% of whom are women.[11] At some point restrictions on return to work because of health status will undoubtedly impact diversity in the workplace. Moreover, as will be discussed more below, employers must be mindful of favoring employees who have recovered from the disease or may display some sort of immunity, under the still yet-to-be-proven belief that an individual who has developed anti-bodies to the virus may have some level of immunity to future instances of the virus.

HIPAA May Apply and Other Laws Which May Serve as a Data Privacy Trap for Employers

It is a common misconception that personal "health information" is automatically protected by the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA is a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without

[5] See EEOC (8 September 2020) What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Accessed September 12, 2020 at https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

[6] *Id.*

[7] *Id.*

[8] The EEOC has definitively stated that "for those employees who are teleworking and are not physically interacting with coworkers or others" an employee is generally not permitted to ask questions about symptoms associated with COVID-19, exposure, or testing for the virus. *See* EEOC (8 September 2020) What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Accessed September 12, 2020 at https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

[9] The Center for Disease Control (24 July 2020) Health Equity Considerations and Racial and Ethnic Minority Groups. Accessed September 12, 2020 https://www.cdc.gov/coronavirus/2019-ncov/community/health-equity/race-ethnicity.html.

[10] The World Health Organization COVID-19: vulnerable and high risk groups. Accessed September 12, 2020 https://www.who.int/westernpacific/emergencies/covid-19/information/high-risk-groups.

[11] Fairweather, DeLisa and Rose, Noel. (10 November 2004) Women and Autoimmune Diseases. Accessed September 12, 2020 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3328995/.

the patient's consent or knowledge.[12] Only health plans, health care providers, and health care clearing houses are subject to the provisions of HIPAA Security, Privacy and Breach Notification Rules. Any other business collecting health related information may not be subject to the privacy regulation, particularly in an emergency situation such as COVID-19, where HIPAA dictates that disclosure of health related is permitted to public health officials.[13]

As of September 8, 2020, at least twenty-six (26) states have required some form of health screening for reopening business. These state mandates to perform symptom screening do not address the issue of protecting the screening information which an employer may collect through a symptom checker application or require adherence to state law. However, there are several existing laws that provide some level of protection for application users that employer should be familiar with.

First, the Federal Trade Commission protects consumers' rights and prohibits companies from engaging in deceptive or unfair acts or practices in or affecting commerce. Among other things, this means that companies may not mislead consumers about what is being done with their personal information, including health information.[14] Also falling under the FTC umbrella is the Health Breach Notification Rule.[15] The Rule requires vendors of personal health records[16] and related entities to notify consumers following a breach involving release of unsecured information.

If HIPAA does not apply and a consumer lodges a complaint with the FTC, the agency may opt to assert jurisdiction. Consequently, where an employer requires employees to utilize an application that collects private data, and that data is used in a manner inconsistent than the notice provided regarding use to the employee (, the employer may be implicated and subject to federal oversight. Recall the Android application study conducted by the IDAC discussed above suggesting that one of the greatest vulnerabilities of these types of applications is that the data collected could easily be transmitted or sold to an unintended party. Thus, it is important to point out that where an employer allows for an app developer or a to sell or transmit that health information collected about employees to third-parties through the COVID-19 symptom checker app, the FTC may opt to exercise its authority, up to and including levying civil monetary penalties. Therefore, it is key for employers to understand what they are consenting to when they agree to an app developer's Terms and Conditions to understand and appreciate the risks associated with any given technology or application. Employers may be best advised to consult with legal counsel about their choice of technology and how to properly communicate the risks and mitigation strategies that employees and customers who will be using the app can employ to protect themselves and their information.

In addition to the federal laws enforced by the FCC, state consumer protection laws may also apply to the applications that employers are and will be using to safely reopen their businesses. Several states have recently enacted measures which require safeguards for private information. For example, the California Consumer Protection Act ("CCPA") requires that an employer provide notice to employees prior to scanning their temperatures and that the employer provide notice to employees about how it will collect the health data and describe each purpose for which the employer will use the information collected. Notably, the CCPA also permits employees to opt out of the sale of their private information and requires that they have the ability to delete any private information collected.[17] Similarly, New York has enacted the New York Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"), requiring any person or business owning or licensing computerized data that includes the private information of a resident of New York ("covered business") to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information.[18]

[12] Dept. of Health and Human Services. What does HIPAA Privacy Rule Do? Accessed September 12, 2020 https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html.

[13] 45 CFR §§ 164.501 and 164.512(b)(1)(i).

[14] See Federal Trade Commission SHARING CONSUMER HEALTH INFORMATION? LOOK TO HIPAA AND THE FTC ACT. Accessed September 12, 2020 https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act.

[15] 16 CFR § 318.

[16] Personal health record is defined as an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." For example, if you have an online service that allows consumers to store and organize medical information from many sources in one online location, you're a vendor of personal health records. You're not a vendor of personal health records if you're covered by HIPAA. Accessed September 14, 2020 at: https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

[17] See California Department of Justice California Consumer Privacy Act (CCPA). Accessed September 12, 2020 at https://oag.ca.gov/privacy/ccpa.

[18] See New York State Senate Bill Senate Bill S5575B. Accessed September 12, 2020 at https://www.nysenate.gov/legislation/bills/2019/s5575.

While the New York law does not permit a private right of action, a complaint lodged regarding the Act is enforceable by the New York State Attorney General. Currently there are twenty-three states and territories which have laws triggering notice to employees on lost, hacked, stolen or other unauthorized disclosure of health information.[19]

The Potential for a Rise in Discrimination Claims

There are several laws which provide protection to employees against discrimination for testing positive for COVID-19 or quarantining as a result of exposure to COVID-19 under the Family Medical Leave Act, Fair Labor Standards Act and the ADA.[20] Overall, employers may see a rise in lawsuits from employees in designated classes asserting that they were denied available hours, subjected to refusals to hire, or terminated because of increased fears of absenteeism or inability to work or who are unable to obtain child care for children out of or in virtual learning programs.

As the American Bar Association Journal points out, one of the biggest legal risks for employers may arise from good rather than bad intentions. Employers, out of concern for the health of older, pregnant, or at risk employees , may be telling or urging them to work from home rather than return to the office, in order to reduce their risk of contracting COVID-19 , while allowing or requiring younger workers or workers who the employers believe to less at risk back to the office.[21] Moreover, the Age Discrimination in Employment Act ("ADEA") - which generally forbids employments discrimination against employees who are 40 and over – does not require employers to accommodate workers who prefer telework because of the heightened impact of the virus on older Americans.[22] To date, the EEOC has not released any data showing the percent uptick in age or disability discrimination claims since the advent of the pandemic.

The data collected from COVID-19 symptom checker applications can lend to this issue exponentially as access to data often informs employer decision making and can lend to claims that employment decisions in hiring, reduction in force, workforce allocation, and termination were made disparately.

Takeaways and Recommendations for Best Practices

In general, employers are left with little certainty regarding the extent of potential liability they may face for sharing or using health information collected regarding employee exposure and testing for COVID-19. Consequently, appropriate review should be undertaken of any application and its related polices engaged by the employer to assist with collecting needed COVID-19 symptom information; additional appropriate steps should be taken to protect the information collected; and all levels of management within a business must receive appropriate training on appropriate subjects to inquire, discuss and utilize in the hiring, firing, and general workforce management context.

Employers should carefully review and understand the Terms and Conditions of any applications they are considering utilizing to thoroughly vet the presence of SDKs in the application before deciding on an application. Employers should also understand how to clearly and transparently communicate to their employees what information the employee is agreeing to have collected through the app. The FTC 's cites the fair information practice principles ("FIPPs") as guidelines that represent widely accepted concepts concerning fair information practice in an electronic marketplace.

---

[19] Alabama, Arizona, Arkansas, California, Colorado, Delaware, Florida, Illinois, Maryland d, Missouri, Montana, New Hampshire, New York, Nevada, North Dakota, Oregon, Puerto Rico, Rhode Island, South Dakota, Texas, Virginia, Washington, and Wyoming.

[20] See Department of Labor, Families First Coronavirus Response Act: Questions and Answers. Accessed September 12, 2020 https://www.dol.gov/agencies/whd/pandemic/ffcra-questions. See also EEOC (8 September 2020) What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Accessed September 12, 2020 at https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws and various state laws.

[21] Meyer, Harris. (1 September 2020) A flood of age discrimination lawsuits is expected from COVID-19 and the economic downturn. Accessed September 12, 2020 https://www.abajournal.com/web/article/flood-of-age-discrimination-suits-expected-with-pandemic-economic-downturn.

[22] See EEOC (8 September 2020) What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Accessed September 12, 2020 at https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

Employers should be mindful to select and use apps that only collect the information that is actually needed. Care should also be taken to ensure that: the information collected is only used for purposes specified to the employee (this also applies to third party SDK collection of data); individuals should be able to find out what information was collected and have access to the information, To this end, employers should pay attention to indemnification and data protection clauses in the terms and conditions of any developer controlled applications. These terms will define the employer's rights if there is unauthorized access to employee health data and will control who will face liability for the unauthorized access or use. To limit liability, employers should carefully choose the COVID-19 symptom tracking app that they use but stop short of requiring its use and provide other avenues for data collection to employees who aren't able to use the app or equipped with a cell phone or mobile device.

The ADA requires that all medical information, such as symptoms of COVID-19 or diagnosis (test results, temperature screening logs, questionnaires and other solicited health information) be maintained as confidential. An employer should make sure that third parties, vendors, and contractors understand this confidentiality concern and limit the number of eyes with access to sensitive medical information.

In terms of workforce management, management should be provided with appropriate training on permissible subjects and discussions at work related to COVID-19. Any and all testing and medical inquiries should be performed in compliance with ADA and EEOC guidelines and uniformly applied. Employers should also ensure that all screening and decisions related to screening are done in a consistent manner to avoid discrimination claims based on protected classifications.

Finally, employers should consider what happens as the pandemic continues and the developers of applications to support health screening potentially adapt and begin to collect additional types of data. The capability of particular applications may well evolve as the need for data related to COVID-19 and its prevention evolves and vaccines are approved and introduced. For these reasons, employers should consider limitations on the length of time which they engage a specific application periodically review their suitability and continued use as circumstances change.

Ryann McKay Hooper is an Associate in the Employment, Labor & Workforce Management practice, in the New York office of Epstein Becker Green. She focuses her practice on representing employers in all aspects of labor and employment law.

Karen Mandelbaum is a Senior Counsel in the Health Care and Life Sciences practice, in the Washington, DC, office of Epstein Becker Green. She has deep experience in all aspects of data privacy and protection due to her work as a privacy and security official at the Centers for Medicare & Medicaid Services (CMS), and in the private sector.

Steven M. Swirsky is a Member of the Firm in the Employment, Labor & Workforce Management and Health Care & Life Sciences practices, in the New York office of Epstein Becker Green. He is a member of the firm's Board of Directors and Co-Chair of the firm's Labor Management Relations practice group. He has devoted his practice almost exclusively to aiding employers in developing strategies to remain union-free and, in organized operations, to securing and expanding management rights in collective bargaining and in proceedings before the National Labor Relations Board.