Employers Considering The Use Of Wearables To Combat COVID-19 Need To Anticipate Privacy Considerations

Insights
6.01.20

As states begin to reopen and businesses that were shuttered for some time plan for a return to work, many employers are faced with the challenge of determining how best to create a safe work environment for employees. In order to enforce social distancing requirements and ensure that employees maintain a safe distance from one another in the workplace, some employers have considered the use of wearable technology.

Wearable Tech Options

There are several options for wearable devices. One such device is a Fitbit-style bracelet worn by employees that creates a virtual bubble of a specified radius. It alerts employees through light and sound if they are encroaching on the predetermined safe range a nearby employee. The data collected by the device is available to employer and employee alike through an online portal, providing information that can help employees consider whether and how to adjust their behavior. Employers receive feedback to help determine whether to adjust work patterns and enable additional employees to safely return to work. The same information could potentially be used for contact-tracing purposes.

Another wearable option is a Bluetooth-enabled device that can be worn as a bracelet or as an attachment to a glove. One such device employs scanning technology, using data transmitted to a downloaded app to a scanner worn in the employee's glove. Both alert employees if they are not maintaining a safe distance from one another.

Wearable technologies such as these could easily be employed in a number of industries. Recently, it was reported that dockworkers at a location in Antwerp, Belgium are beginning to use wearable bracelets originally designed to enable workers to call for help if another employee fell in the water or suffered an accident. The bracelets have been adjusted to alert workers if they are less than five feet apart. The manufacturer envisions the potential use of the devices in other industrial settings. Some wearable manufacturers have announced an intention to market the devices to food manufacturers, construction companies, food manufacturers, and those in warehouse settings.

Recent reports have suggested that traditional wearable fitness trackers could offer additional tools, beyond social distancing measures, to identify employees who may be exhibiting early symptoms of COVID-19. Within the last two weeks, in fact, Fitbit announced the launch of its own COVID-19 study,

available in its app, to help determine whether the company can build a reliable algorithm to detect COVID-19 before individuals may even present observable symptoms.

Wearables Raise A Host Of Privacy Concerns

As with other employee screening technologies, the availability of wearable devices to track employee movement and potentially identify early symptoms of COVID-19 presents privacy concerns and challenges for employers. The issues presented by these devices vary depending on the technology they employ and the data they collect. Employers evaluating the possible use of wearable technology should begin by asking the following questions:

- What data is collected by the device?
- Where is the data stored?
- How long is the data maintained?
- Who would have access to the data?
- Does the employer have the ability to limit/control the above?
- If the data is maintained by a third-party vendor, what security measures does the vendor employ? Will the data be used/shared for any other purpose?

Other considerations include whether the employer will provide the device, if there is an associated app, and whether the employer will ask employees to download the app to a personal phone or one provided by the employer. If loaded onto a personal device, another consideration would be how the employer will manage situations in which an employee either does not own a personal device that would support the app, or simply refuses to download the app or use the technology. Yet another consideration is how an employer will accommodate an employee who may raise an objection to using wearable technology for health or medical reasons, such as an allergy or disability that makes the use of the technology difficult or impossible under the circumstances. The use of technology to enforce social distancing measures, or to identify employees exhibiting symptoms of COVID-19, becomes less viable if multiple employees are not using it.

To increase the likelihood that employees who are able to use wearable technology will agree to do so, it is critical that employers obtain and share information regarding the method by which the technology will be employed, as well as the type of information that will be collected, how the information will be used and maintained, and who will have access to it. Additionally, employers may be required to provide notice of the information collected. For example, the California Consumer Protection Act (CCPA) requires employers to notify employees of personal information they are collecting and the business purpose for which it is being collected. Even where there is no statutory obligation to provide such notice, employees who learn that personal data was collected without notice through a wearable device could potentially assert claims for invasion of privacy, among other things.

Dangers Of Data Breaches And Cyberattacks

A number of states also define medical and health information as personal information that is subject to data breach notification laws. This means that if personal information is being collected and stored, and that information is hacked or otherwise breached, the employer would have an obligation to notify employees of the breach. The employer may also have liability if it did not take adequate measures to ensure that the data being collected was securely maintained. This could be in the form of fines, or civil litigation, where permitted under data breach notification laws, or under negligence theories. In California, pursuant to the CCPA, this could mean potential recovery of damages in a civil action of $100 to $750 per person, per incident, or actual damages, whichever are greater. The California Attorney General also has discretion to prosecute companies for violations of the CCPA, and may impose penalties of up to $2,500 per violation, or $7,500 for each intentional violation.

Already, there have been numerous reports and warnings regarding the significant increase in cyberattacks since the onset of the COVID-19 pandemic. These are likely to continue, and it is conceivable that attacks will be directed at apps and databases that may store employee health or other personal information. As many of the technologies being offered are new and may be relatively untested, it is critical that employers take precautions before deploying new wearable technology to identify the method by which any data being collected will be secured and protected against potential cyberattacks. This should include making a detailed inquiry of any potential vendor, and carefully reviewing and negotiating contractual terms to both identify security measures and, to the extent possible, require indemnification and address the duty to defend any litigation that may be brought as a result of the compromise of a vendor's systems.

To the extent data is being collected, employers should endeavor to ensure that the system being employed maintains the data for only a limited amount of time, which reduces the risk that it could later be hacked and disclosed to third parties. Additionally, access to data should be limited to the fewest individuals necessary, and employers should consider whether health or medical information should be available only to the employee wearing the device, rather than the employer. In that circumstance, employers may couple the device with a request that employees notify the employer if symptoms of COVID-19 have been detected, as would be the case with a temperature check or the onset of other symptoms of the virus, even without a wearable device.

Final Considerations

For the most part, employers will not be subject to HIPAA restrictions with respect to the collection of data through wearable devices, as HIPAA privacy restrictions only apply to "covered entities" such as medical providers or employer-sponsored group health plans, and then only in connection with individually identifiable health information. Employers are typically not covered entities, so medical information collected through wearable technology would generally not be subject to HIPAA restrictions. However, if an employer operates a self-funded health plan and collects health information through an app associated with a wearable device, HIPAA rules and regulations regarding the use and disclosure of personal health information (PHI) would likely apply. If that is the case, employers should seek legal advice to ensure adherence to applicable requirements.

Finally, for devices like those being deployed to dockworkers in Belgium, which merely alert employees who come within a certain distance of one another, employers may be able to minimize privacy concerns by ensuring that devices do not employ or store geolocation data. As is reportedly the case with the devices being used in Belgium, some devices are designed to merely communicate with other devices to provide necessary alerts while employees are at the employer's worksite, without collecting or storing any data.

Conclusion

As wearable technology develops, it may eventually provide a viable solution for many employers to facilitate the early detection of COVID-19 symptoms, and to enforce social distancing measures to reduce the risk of infection in the workplace. The use of these technologies presents both promise and potential privacy concerns. To maximize the benefit from these devices, while reducing privacy risks and reassuring employees of the safety and security of wearable devices, employers should take steps to ensure that they have a strong understanding of the technology employed and data collected, and how it is maintained and secured.

A comprehensive understanding of these issues, coupled with an appropriate disclosure and notification to employees, will help to maximize potential benefits and reduce legal risks. It will also enhance the likelihood that employees will feel a measure of comfort in using wearable technology to combat the risks associated with a return to work in the COVID-19 environment.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Service Focus

Privacy and Cyber