Featured Professionals

Megan A. Bowman, CIPP

Sten-Erik Hoidal, CIPP

Related Services

Data Protection & Cybersecurity

Employment, Labor & Benefits

Technology & Data

Question of the Day: Privacy Considerations for Protective Health Measures

Legal Update
06.05.2020

By Sten-Erik Hoidal and Megan A. Bowman

Question

Do I need to worry about employee privacy if I implement health screenings, contact tracing or similar protective measures when my employees return to work?

Answer

As stay-at-home orders ease in many states, businesses are preparing to return employees to work and developing plans and policies for addressing the persistent threat of COVD-19 in the workplace. Many technology companies are offering solutions to help business address this threat, such as employee monitoring apps that aid contact tracing or thermal cameras that assess employees' temperatures. Use of these technologies present potential employee privacy issues that employers will need to navigate as they implement their strategy for confronting the continuing threat of COVID-19.

What laws apply?

Unlike Canada and the European Union, the U.S. does not have an overarching federal legal framework that governs data privacy. Rather, privacy is addressed either at the state level, with laws like the California Consumer Privacy Act (CCPA), or with industry- or sector-specific laws, such as the Health Insurance Portability and Accountability Act (HIPAA), Americans with Disabilities Act (ADA) and Fair Credit Reporting Act (FCRA). The applicability of a specific privacy law often depends on the type of personal information collected, the location of the individual to whom the information relates, the source of the information or how the information is used.

For example, HIPAA applies only to covered entities—which include health care providers, health plans and health care clearinghouses—and their business associates. In most cases, HIPAA does not apply to a business' data collection and privacy practices if the business is acting as an employer. On the other hand, the California Consumer Privacy Act (CCPA), governs the collection of any information

that can be used to identify a California resident, including geolocation, biometric or visual data, and can apply to businesses outside of California, provided they meet certain applicability thresholds.

Are you required to obtain certain consents or provide certain notices before taking employee temperatures or engaging in employee contact tracing?

Whether employers are legally required to provide notice to or obtain consent from employees for return-to-work screening measures depends on which privacy laws apply to the employer. For example, the Illinois Biometric Information Privacy Act (BIPA), which regulates the collection and storage of biometric information from Illinois residents, requires businesses obtain informed consent prior to the collection of such information. Similarly, the CCPA (discussed above) requires qualifying businesses provide California employees notice of the company's practices at or before the time the company collects personal information from those employees. Both of these laws, of course, contain exceptions that may apply to the company or the specific information being collected.

Companies will need to analyze the specific privacy laws that apply to their collection of personal information from employees in connection with COVID-19 screening and mitigation efforts. Nevertheless, informing employees about the screening measures, the types of personal information that will be gathered, and how it will be used, and obtaining employee consent for the measures, can be helpful practices regardless of whether they are legally required.

Do your vendor contracts appropriately address data privacy?

If employers use an app or a vendor to assist with return-to-work screening processes, they should evaluate how the vendor intends to use the information and what the vendor is doing to maintain the security and privacy of information. It is essential the employer ensure that the vendors with whom it contracts are safeguarding personal information appropriately and only using it for the purposes of performing the contracted-for services. Indeed, under some laws, the employer is required to do so. The EU's General Data Protection Regulation (GDPR), for example, requires certain provisions in contracts between the businesses who collect and direct the processing of personal information and the service providers or vendors who process, transmit or store the information on the businesses' behalf.

What can you do to reduce your risk?

One way to reduce your risk is to limit the amount of personal or sensitive information you collect. For example, consider anonymizing temperature screenings so that they are not associated with a particular employee. Also, limit access to personal or sensitive information to only those who need to access it. Finally, and most importantly, develop and document procedures for the handling of personal information collected through return-to-work screenings. Doing so will help crystallize

what information is being collected, how it is being used, where it is being stored and who has access to the information.

Takeaway

Proactive and thoughtful planning is key to successful, comprehensive and cost-effective privacy compliance. Accordingly, as companies develop their return-to-work strategies, they should partner with counsel to make sure they understand the privacy implications and compliance requirements associated with employee screening and personal information collection.

If you have questions or need assistance, contact your Fredrikson & Byron Data Protection & Cybersecurity attorney.

View All: COVID-19 Employment Question of the Day