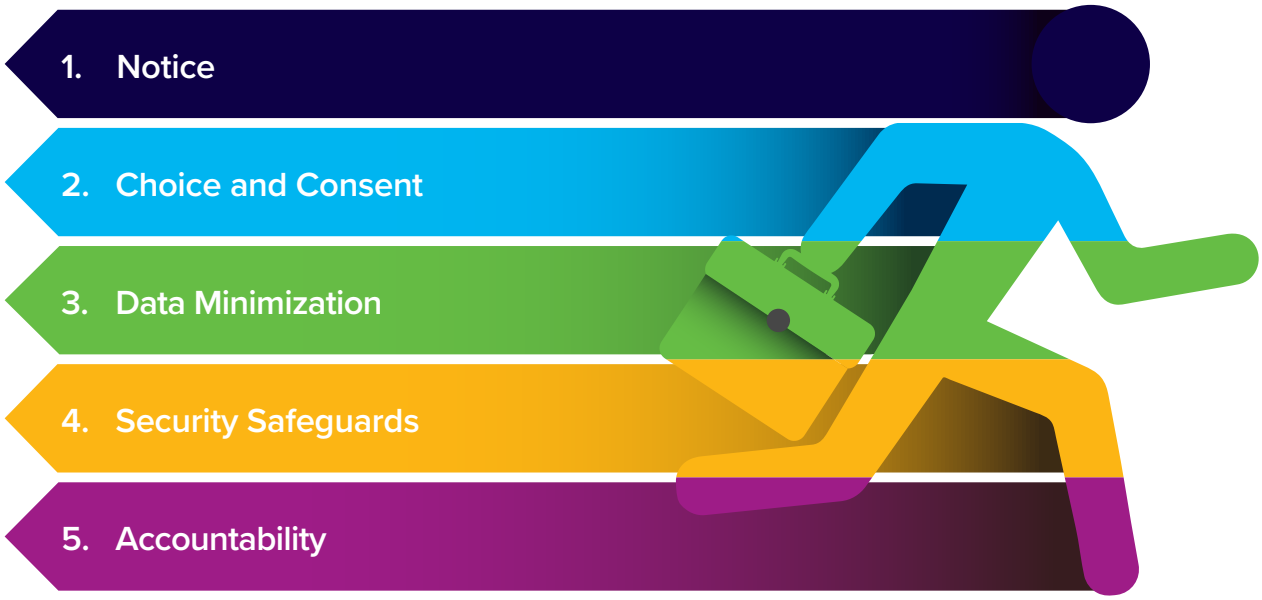
Notice to Employers: Remember Privacy Basics When Addressing COVID-19

troutman sanders

As the coronavirus (COVID-19) continues to spread, businesses are pushed to make swift decisions that impact not only business operations, but also the privacy and security of employees' personal information. In times like these, the Fair Information Practice Principles (FIPPs) should be every organization's guiding light.

The FIPPs are principles that address the privacy of individuals' personal information and provide the foundation for many U.S. state and federal privacy laws (e.g., the California Consumer Privacy Act [CCPA] and the Health Insurance Portability and Accountability Act [HIPAA]) and international privacy laws (e.g., the General Data Protection Regulation). When decisions have to be made under pressure, businesses would be wise to refer back to the FIPPs as a sounding board prior to taking action. Below we highlight a few core privacy principles that should be at the forefront of every organization's thinking as the organization tackles the operational effects of COVID-19.



1. Notice

Many articles and guidance have been issued on whether employers are able to collect certain employee information in light of COVID-19 concerns (e.g., body temperatures to test employees/customers/guests for symptoms, inquiries that may reveal employee disabilities or medical conditions). The Equal Employment Opportunity Commission has stated that employers may ask about an employee's symptoms and take employee temperatures in the event of a pandemic. Under "normal" circumstances, however, taking an employee's temperature constitutes a medical examination under the Americans with Disabilities Act and would only be permissible if job-related and consisted with business necessity.

Notice, a fundamental privacy principle, requires notice before any personal information is collected. Notice allows individuals to make an informed decision as to whether they want to provide the information requested. Many privacy laws mandate these types of "just-in-time" notices including, for example, the CCPA and HIPAA.

Employers should carefully consider how best to provide notice under the circumstances. For in-person collection, consider providing the notice in paper form and documenting the fact that it has been provided. If collecting information through other means (e.g., online or by phone), the minimum should be an email notice with a "read receipt" requested and logged. While some laws may provide flexibility in providing notice in light of emergencies (e.g., in certain emergency treatment situations, HIPAA provides flexibility when providing the required notice), other laws may not be as generous. As such, it is recommended that all businesses review their employee privacy notices to determine what data collection and usage practices have been previously disclosed and issuing revised notices in light of the circumstances, if need be.

2. Choice and Consent

Another core privacy principle is individual choice and consent. With many moving to remote work environments, businesses should consider when consent to collect or access personal information is being freely provided, or if consent is obtained because the individual simply has no other choice.

For example, consider employees who are required to use personal devices to work from home. Many businesses may require employees to submit their devices beforehand to scan for malware or install security applications. Businesses may even ask or require as a condition of using their own devices that employees agree to having their devices remotely accessed or wiped. When operations return to "normal," businesses may again require employees to submit their devices for security scanning. While taking these steps, businesses may access employees' personal information that they would not otherwise access.

Companies should consider whether employees are voluntarily consenting to the collection of their personal information. If possible, businesses should issue their own devices for remote work arrangements rather than asking employees to use their own. If that is not an option, businesses should, at a minimum, provide adequate notice of what information they may access and how such information will be used. Any processing that is not compatible with the purpose for which the information was accessed or collected will raise additional issues (e.g., using information collected during a scan as evidence that an employee violated the company's acceptable use policy). Where the only option is to consent, adequate knowledge will be key.

3. Data Minimization

If businesses are collecting new types of personal information as a result of the COVID-19 outbreak, businesses should only collect information needed to address their valid and lawful concerns. For example, although employers may be justified in asking about an employee's travel history or if they have experienced COVID-19 symptoms, it may not be reasonable to ask questions about employees' off-duty activities or medical history, family members' medical issues or activities, or other information that could lead to the discovery of a disability.

Limiting the scope of inquiry is in line with the FIPPs "data minimization" principle, which provides that there should be some limits to the collection of personal information, and any such collection should be directly relevant and necessary to accomplish the specified purpose(s). Businesses may also want to consider only retaining the information as long as necessary or as otherwise required by law.

4. Security Safeguards

With many businesses moving to a remote-work environment, businesses should reiterate the importance of safeguarding confidential information and systems, including personnel information. The security safeguards principle provides that personal information should be protected by "reasonable" security procedures to protect against unauthorized access, destruction, use, modification or disclosure of data.

While what constitutes "reasonable security" during a pandemic is still being defined, businesses should assess what safeguards are needed in light of new work-from-home environments (see Troutman's publication, "COVID-19 Warrants Modified Cybersecurity for Work-at-Home," for additional information).

For example, for physical security, businesses may remind employees to lock screens when not in use or that the "clean desk" policy also applies at home. Businesses should also assess risks of information storage and disposal, which will be most prevalent if physical or paper files are brought home or if information is being stored locally or on portable devices. For technical security, businesses may want to consider requiring multi-factor authentication and requiring employees to use only encrypted communications and provide a list of at home security improvement (e.g., strong router password).

Given the number of IT issues employees will likely encounter when shifting to remote work, businesses should also consider requiring authentication before receiving calls from helpdesks or otherwise to avoid pretexting/phishing. For additional information on this topic, see Troutman's publication, "Cybersecurity Tips to Prevent Your Business from Becoming COVID-19's Virtual Victim."

5. Accountability

Core privacy principles can only be effective if there is a mechanism in place to enforce them. Given how quickly new practices and procedures are being rolled out, businesses should consider creating a "COVID-19 Resource Center" to document the new, but likely temporary, notices, policies, and procedures. A central access point will make it easy for employees to locate and reference any new policies while allowing the organization to keep track of what policies it implemented and updated during this period. This will be especially important for when operations return to "normal" and businesses need to claw back on temporary measures.

For privacy and cybersecurity issues, contact Ronald I. Raether at ron.raether@troutman.com. For issues relating to employment law, contact Mark Payne at mark.payne@troutman.com.