Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Employers Face Privacy Balancing Act In Coronavirus Fight

By **Allison Grande**

Law360 (March 12, 2020, 10:07 PM EDT) -- From checking temperatures at the door to letting employees know a colleague is sick, companies are grappling with how to strike the right balance between personal privacy and public safety in their response to the coronavirus pandemic, and a familiar privacy principle could provide a lot of help.

The novel coronavirus is putting to the test the recent global trend toward laws that give consumers more privacy rights, forcing employers to make quick decisions about what personal information they need to collect to protect their workforce.

"Those are really hard privacy questions, and there are a lot of different angles that need to be considered in answering them," said Lynn Sessions, a Houston-based partner who leads BakerHostetler's health care privacy and compliance team and is a member of the firm's coronavirus task force.

Most privacy laws contain narrow exceptions for public health and safety purposes, including the European Union's General Data Protection Regulation, which covers essentially all businesses that process health data, and the U.S.' Health Insurance Portability and Accountability Act, whose application is generally limited to health care providers and their business associates.

But while the carveouts may give some cover to health care providers and employers, particularly when it comes to sharing information with public health officials, companies still need to put reasonable limits on these activities, attorneys say.

"If an employer is reaching out to an employee for personal information, it needs to determine what information is really necessary in order to take steps to tackle and assess the risk and to protect other employees," said Eduardo Ustaran, a Hogan Lovells partner based in London. "And if an employer needs to tell others about a colleague who's tested positive, it needs to consider whether disclosing information like that person's name is necessary."

"It's really important to have a sense of proportionality, and a guiding principle should be that if information is not really necessary to be collected or disclosed, it shouldn't be," he added.

Familiar Challenges in Uncharted Waters

Calls started flowing in from clients last week concerning plans to stop employees and visitors at the

door, take their temperature and request other health information from them — and turn them away if they showed any signs of the virus, according to Cynthia Cole, a California-based special counsel to Baker Botts LLP.

Fever, coughing and shortness of breath are some of the most common symptoms of coronavirus, which causes the disease known as COVID-19.

"My first response was, 'I'm glad you contacted me,'" Cole said.

These efforts to limit the spread of the virus raise questions such as what's being done with the information being collected, whether temperature readings are being written down, how broadly this information is being shared and who's responsible for enforcing exclusion orders, according to Cole.

The issues are somewhat similar to those presented by the response to the Sept. 11, 2001, terrorist attacks, which raised the same questions about the extent to which individual privacy should be curtailed in the name of public safety, Cole added.

Some employers have also started distributing health check surveys requesting a range of information about not only their employees, but also the people they live with, said Jim Koenig, a New York-based partner who co-chairs the privacy and cybersecurity practice at Fenwick & West LLP.

"When questions start moving beyond employees and become about others in the house, that starts getting more complicated," said Koenig, who recommended that companies make it optional for employees to answer those questions.

Employers also face a dilemma over how much to tell employees about a colleague who has tested positive for the virus, with attorneys generally advising companies keep such revelations nonspecific, but not to the extent it deprives workers of useful information.

"There's always a caution about sharing a person's name, but by the same token, companies want to ensure that the rest of the employee population is able to appropriately protect themselves and their loved ones, so that's a judgment they'll have to make," said Sessions, the BakerHostetler partner.

These tricky decisions can be aided by a principle known as data minimization, which emphasizes collecting only what's absolutely necessary to perform the task at hand. This concept has long been established in the privacy world and factors prominently into laws such as the GDPR and the California Consumer Privacy Act.

Emerging privacy laws also generally require companies to undertake impact assessments to identify what information they hold and the risks of maintaining or disclosing that information — an exercise that is likely to help companies address privacy risks posed by their coronavirus response efforts, attorneys say.

"It's not unlike a data privacy assessment, where companies are faced with a new issue and need to look at the situation from a wide-angle lens to understand whether they have the right framework in place to bring in this personal information in a way that creates the least amount of risk and delivers the most benefits," Cole said.

Companies may also be able to rely on some of the "muscle memory" they've developed from responding to cyber threats and other incidents in recent years to navigate these concerns, according to David A. Newman, a Washington, D.C.-based partner at Morrison & Foerster LLP who leads the firm's coronavirus task force.

"A lot of the same theories and principles that apply in cyber incidents apply in this situation, including having to bring in experts and decision-makers together to address the issues and making sure the correct notifications and disclosures are being made," Newman said.

But while the privacy questions confronting companies dealing with the coronavirus outbreak are far from foreign, "the novel issue lies in how rapidly the landscape is changing, and therefore how fast organizations are being required to react to employment, data protection and commercial issues," Ariane Mole, a Paris-based partner who co-heads Bird & Bird LLP's international data protection practice, and Clara Clark Nevola, a U.K.-based attorney in the firm's privacy and data protection group, said in a joint email.

"The COVID-19 situation is evolving rapidly," they added.

This means that, unlike the significant lead time companies had to get up to speed with privacy obligations under the GDPR and CCPA, employers who aren't generally accustomed to asking employees about their health histories or reasons for calling out sick will be pressed into snap decisions with serious implications.

"We're getting questions from global clients that want to know whether they can ask for and share certain personal information, and they can't wait a week or two for an answer," Ustaran said.

Making a Plan

The best course of action for companies will likely be to develop a clear plan in conjunction with guidance that authorities and regulators are beginning to release for collecting and disseminating personal data, and to make sure those rules are being applied consistently.

"It's about striking a balance, because everyone wants to stay healthy, but not necessarily at the cost of compromising personal privacy," Koenig said.

Companies also need to be ready to revise their strategy as circumstances change, according to Newman, who before joining Morrison & Foerster served in government roles that included chief of staff for the White House's Ebola response efforts during the Obama administration.

"One of the lessons from the Ebola response is that there's a lot of unpredictability, and we're constantly learning new things about how the virus spreads," he said. "So companies need to be working quickly to fashion response plans, but also need to be prepared for the fact that information and risks can change quickly and adjust their approach based on a very evolving landscape."

The World Health Organization — which on Wednesday said the coronavirus was now a global pandemic — has documented more than 125,000 cases of infection in 118 countries worldwide, with over 4,600 deaths since it emerged in Wuhan, China, late last year.

Several regulators in the EU, including data protection authorities in Italy, France and Ireland, have in

recent days offered somewhat contradictory guidance on where the lines should be drawn when it comes to collecting, sharing and using health data in connection with the virus.

The data protection regulator in Italy, which has been hit particularly hard by the virus, advised companies to refrain from undertaking "autonomous initiatives" — including making specific requests to individual workers — to collect information about workers' current health status, their contacts or life outside of work.

The French authority, CNIL, similarly advised against collecting data that would "go beyond the management of suspected exposure to the virus," and explicitly came out against the practices of recording employees' or visitors' temperatures and distributing medical questionnaires.

On the other end of the spectrum, Ireland's Data Protection Commissioner has said that while data processing activities need to be necessary and proportionate, employers may be justified in asking employees and visitors about their travel histories and whether they're experiencing symptoms in order to meet their legal obligation to maintain a safe workplace.

While the guidance is instructive, "what would be helpful is to have some harmonized guidance across the EU," Ustaran said, noting that the European Data Protection Board, a collective of the national data protection authorities from each member state, has yet to weigh in on the issue.

Cyber Hygiene Is Important Too

As companies collect more personal health information to try to contain the virus' spread, they need to be mindful they're applying the same data security protections to this information as they already apply to other personal information, attorneys noted.

"Companies need to set up the appropriate safeguards and routines to make sure their information-handling hygiene is as clean as their personal health hygiene so they don't catch a breach along with the spread of the virus," Koenig said.

Moves to empty offices and direct employees to work from home also raise concerns over whether these remote operations are secure — or if they're creating more technological paths of access for increasingly sophisticated hackers, according to Newman.

"Bad actors are no doubt aware of what's going on and are likely looking to try to exploit the cyber risks that arise from letting employees telework," he said.

Attorneys say they expect to continue to hear from clients as these privacy and cyber risks evolve, noting the volume of inquiries they've received to date indicates employers are aware of these issues and taking them seriously.

"This outreach shows that data privacy awareness is maturing within companies, to the point of where they're understanding that the impact of these health privacy issues is much larger than simply the question of whether or not they're covered by HIPAA," Cole said.

--Editing by Philip Shea.