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

Virus Vaccine Tracking To Keep Focus On Data Privacy

By **Allison Grande**

Law360 (March 11, 2021, 8:42 PM EST) -- A year after the onset of the COVID-19 pandemic in the U.S., companies are still grappling with questions about how to handle and retain sensitive health information, and emerging efforts to monitor who's been vaccinated will only exacerbate these issues.

When the coronavirus outbreak was officially declared a pandemic last March, many businesses had to scramble to set up new protocols in order to safely operate, including collecting temperatures and health screenings from customers and employees.

This sudden shift, coupled with the lack of a federal data privacy framework and often conflicting guidance from regulators, left companies with an influx of questions about how to contain the virus' spread without compromising personal privacy.

"It was a whole new world, because organizations typically didn't collect so much health information and in an instant had to start dealing with questions about what they're doing with this information and how long they're keeping it," said Timothy Shields, a data privacy partner in the Fort Lauderdale office at Kelley Kronenberg. "Now, questions related to whether someone's been vaccinated will create a whole new set of challenges."

The novelty of the pandemic, especially in its early days, created widespread "uncertainty and confusion" around data privacy issues since companies didn't have protocols in place or any legal precedence to follow, according to Adrienne Ehrhardt, the chair of Michael Best & Friedrich LLP's privacy and cybersecurity practice group.

"So it was unclear to companies what data they could and should collect and retain, what notices to provide, and what action to take based on that data," Ehrhardt said.

Companies have had to confront a range of privacy issues, including whether the Health Insurance Portability and Accountability Act or some other regulatory framework applied to the sensitive health data being collected, how much they could disclose to health officials and employees about positive results, how long they should keep this information, and to what extent this data could be anonymized.

As companies have gotten more accustomed to collecting health and contact tracing data during the past year, many have found that information like temperature checks don't need to be tied to specific individuals or held onto for more than a couple weeks, according to attorneys.

But keeping track of whether employees and visitors are vaccinated, or even requiring the vaccine for entry, will require a more personalized inquiry that will likely carry additional legal risks, attorneys say.

"The compromise we've reached with the retention of health questionnaires, testing and temperature checks, we can't do that with vaccine data, since the whole idea is that you need to know if a specific individual is vaccinated in order to get on an airplane or come back to a workplace," said Miriam Wugmeister, partner and co-chair of Morrison & Foerster LLP's privacy and data security practice.

Companies' move to collect more data in the wake of the pandemic has exposed them to increased liability under an emerging patchwork of data privacy laws, including the California Consumer Privacy Act and the European Union's General Data Protection Regulation, which require companies to be more transparent about the personal information they're collecting and aim to give consumers more control over how it is used and shared.

But while policymakers are trending toward instituting more protection for the use and disclosure of data like health information, including requiring opt-in consent, that consideration has gotten "flipped on its head with a highly infectious disease such as COVID that has permeated our society on so many levels and where one person's disease status has a tangible real-world impact on the others around them," noted Hogan Lovells partner Bret S. Cohen.

"At the same time, age-old privacy concerns about individual autonomy and concerns about discrimination are real and cannot be swept aside," he added. "So long-term, the questions about what people can keep private about their health conditions — and what they can be forced to disclose — will continue to be debated."

Employers have also had to be careful with how they've handled workers' information, since that is covered under employment laws that contain different privacy, security and data retention requirements than consumer privacy laws.

"There is much more of a push in the employment law context to retain records, as opposed to the thrust of these new data privacy and security laws, where the preference has been for data minimization," said Greg Szewczyk, a partner at Ballard Spahr LLP.

Therefore, it's become increasingly vital for companies to think about this health check and virus tracking data separately from their treatment of human resources data like background checks and benefits information, which are typically put in a personnel file and become subject to lengthy data retention requirements.

"This health data is being collected for a specific purpose for a limited amount of time, and it's highly personal," said Linn Freedman, a partner at Robinson & Cole LLP. "So companies need to think about it in a different way than typical HR data, because they don't want this information put in someone's HR file forever, and employees would also appreciate knowing that their employer is only using the data for certain purposes and will destroy it."

But even within a single organization, how long information should be retained is not always clear-cut.

During the past year, somewhat unanticipated tension has emerged between privacy professionals who have encouraged the quick disposal of such information and litigation-minded advisers who have

advocated for holding onto it for longer to show the company has taken all reasonable steps to protect its staff and visitors, noted Wugmeister, the Morrison & Foerster partner.

That conflict is beginning to work itself out, with companies in general favoring an approach under which they screen individuals but don't retain detailed results.

"The fear of litigation has come down a few notches, and the privacy issues have become more paramount," Wugmeister said.

This dichotomy is similar to the one that's emerged in the guidance regulators put out during the past year. On the one hand, employment authorities like the U.S. Equal Employment Opportunity Commission give companies leeway to collect data to track the virus without violating existing regulations, while European data protection regulators have trended more toward limiting the data that's gathered and how long it's kept, attorneys noted.

"On a global basis, the guidance on COVID-19 data collection issues has been all over the map," said Wugmeister.

In the wake of this guidance, companies have moved to engage with both their private-sector partners and government regulators to devise a process that balances public safety with privacy concerns.

"The public and private sectors will need to continue harmonizing these somewhat competing interests while also balancing the benefits and risks introduced by data-driven technology solutions," said Elizabeth Rogers, a partner at Michael Best & Friedrich LLP. "A fair balance of post-pandemic individual, public and business interests will depend on all of these actors continuing to work together."

As the pandemic enters its second year, the next frontier, particularly for employers, will be the thorny questions that are already starting to arise over whether businesses can require workers or visitors to be vaccinated and what information they can ask for as proof of this step, attorneys noted.

"With respect to vaccinations, a primary concern is ensuring that any proof of vaccine is limited to just that — proof of vaccination," said Michael Bahar, who co-leads the global cybersecurity and data privacy practice at Eversheds Sutherland. "If an employee refuses to be vaccinated on the basis of protected grounds such as a disability or religion, for example, the company should generally take steps to avoid follow up questions."

Companies should also take into consideration work-from-home arrangements, which are likely to continue into the foreseeable future, in crafting any vaccination policy, Bahar added.

"For example, requiring a work-from-home employee to show proof of vaccine may be an unreasonable intrusion into that employee's privacy, and it may trigger employment law concerns under the Americans with Disabilities Act," he said.

And the unprecedented data collection that the pandemic has brought has heightened an already active drive to institute more data privacy protections for consumers, attorneys noted.

"We've been reminded that privacy is a daily decision of individuals to trade information for what serves their greater need or want," said Arent Fox LLP partner Eva Pulliam. "This sentiment is one that may carry forward in limited circumstances, but is in tension with the broader push for consumer privacy

rights."

California and Virginia have moved to enact comprehensive consumer privacy laws to regulate how companies use, share and sell personal information, including sensitive data, and several other states are expected to soon follow with frameworks that give consumers more insight into and control over what companies are doing with their information.

Federal lawmakers have been pushing for several years to head off this emerging patchwork by creating a national privacy framework, but disputes over the extent that such a law can preempt more stringent standards crafted by states, and whether consumers should be allowed to sue, have derailed these efforts.

Yet Rep. Suzan DelBene, D-Wash., attempted to reignite these efforts Wednesday by proposing legislation to require companies to obtain "affirmative, express and opt-in consent" from consumers before they use or share financial, health, biometric and other types of sensitive data in unexpected ways.

"The current situation with COVID-related data underscores the compelling need for federal action," said Mary J. Hildebrand, the founder and chair of the privacy and cybersecurity team at Lowenstein Sandler LLP. "California residents have been accorded certain rights to personal information under state law which may be helpful, but protection of this sensitive data should not depend on where you live."

Even without a federal standard, the concepts of data minimization and differential privacy are likely to persist, noted Colleen Brown, a privacy and cybersecurity partner at Sidley Austin LLP.

"Like data, trust is a corporate asset," Brown said. "Both can be severely undermined by privacy missteps."

--Editing by Philip Shea and Kelly Duncan.