Simpson Thacher

Memorandum

Strategies for Complying With Privacy Laws While Collecting Employee Information Regarding the Coronavirus

March 23, 2020

Most companies must collect and use information about their employees' travel plans and health conditions to protect their workforce from the spread of coronavirus disease 2019 ("COVID-19"). This memorandum addresses strategies for U.S. companies to comply with various privacy laws in connection with these activities.[1]

HIPAA

The Health Insurance Portability and Accountability Act, as amended by the Health Information Technology for Economic and Clinical Health Act, and the regulations that implement both laws (collectively "HIPAA") govern uses and disclosures of protected health information ("PHI"). PHI includes individually identifiable health information that is transmitted or maintained electronically or in any other form, but excludes such information in certain records, such as employment records held by a covered entity in its role as an employer. HIPAA applies to covered entities: health plans, health care providers who transmit health information electronically in connection with a covered transaction (e.g., the transmission of health care claims), and health care clearinghouses. Business associates and subcontractors must also comply with certain HIPAA requirements. Business associates are persons or entities that create, receive, maintain or transmit PHI on behalf of a covered entity for certain functions or activities (such as claims processing, data analysis, benefit management, and billing) or who provide certain services that involve the disclosure of PHI (such as management, administrative or financial services). Subcontractors are persons or entities to whom a business associate has delegated a function, activity or service. If an employer is not a HIPAA covered entity, business associate or subcontractor, then HIPAA's restrictions on uses and disclosures of PHI do not apply, but the employer must still consider state laws on uses and disclosures of health information and the other laws discussed below.

A HIPAA covered entity's uses or disclosures of PHI, such as an individual's test for the virus responsible for causing COVID-19, must be made in accordance with HIPAA's requirements. For example, HIPAA permits covered entities to disclose PHI to public health authorities or pursuant to an individual's authorization, to disclose PHI for treatment and notification purposes, and to disclose PHI to prevent or lessen a serious and imminent threat to the health and safety of a person or the public. Employers who seek to involve their group health plans in the collection of PHI—other than summary health information or information on participation and

[1] This memorandum provides a high-level summary of each cited law. For a more detailed discussion, please consult one of the authors of this memorandum.

enrollment—must follow additional HIPAA requirements with respect to such PHI that is created or received by the health plan.

If an employer is not a HIPAA covered entity, business associate or subcontractor, HIPAA and other laws may still limit the employer's ability to obtain, use or disclose an employee's health information. If an employee wishes to disclose PHI related to medical care and treatment to their employer, the employee could request that their health care provider (a covered entity) send their employer the results of a COVID-19 test pursuant to a HIPAA authorization for release of PHI. A current, valid authorization would enable the employee's health care provider to disclose the employee's test results directly to the employer.

GINA

Employers should exercise caution when contemplating whether to request or require copies of any COVID-19 test results, so as not to trigger laws that apply to employer practices and "genetic information." The Genetic Information Nondiscrimination Act ("GINA") provides that an employer generally may not request or require genetic information of an individual or family member of the individual, but there are exceptions for certain requests, such as requests for family medical leave. Though the focus of GINA and state laws on genetic testing is genetic tests such as carrier screening and DNA tests to detect genetic markers, the definitions of genetic information or testing may be broad enough to include a COVID-19 test of an individual or family member.

CCPA

The California Consumer Privacy Act, which took effect January 1, 2020, requires covered companies to disclose to all California residents—at the time any of their personal data is collected—what information is being collected and how it will be used. This applies to a company's employees, contractors, directors and medical staff members, if they are California residents. A mass email should suffice to comply with this obligation. Once collected, as with any other personal data held by a company, the company will be liable for damages under the CCPA if a security breach occurs and unencrypted personal data is accessed. The CCPA does not cover medical information governed by HIPAA, and an exception exists for activities necessary to comply with the law and law enforcement agencies.[2]

GDPR

The processing of employees' travel and health-related information may also be subject to the EU General Data Protection Regulation ("GDPR") to the extent such data is, broadly speaking (i) processed by an EU-based company, subsidiary or business or (ii) collected by a non-EU entity regarding employees' activities within the EU (Article 3). The GDPR does not apply to the processing of personal data of EU citizens who reside and work in the United States, because of its territorial scope. However, gathering data about travel and health issues of employees while they are within the EU would be subject to the GDPR.

[2] CCPA, Sections 1798.145(a), 1798.100(b) and 1798.150.

The GDPR allows processing of employees' personal data on various grounds, including (i) with the employee's consent (which can be withdrawn, so this is not the optimal basis); (ii) to protect the vital interests of the employee or other people (which is a very narrow exception that requires an immediate "life or death" situation and no other options); (iii) to carry out a task in the public interest as provided in EU or EU Member State law; or (iv) to pursue legitimate interests of the company or a third party, provided that such interests do not override the fundamental rights of the employee (Article 6). The GDPR specifically states that processing data to monitor epidemics and to prevent or monitor communicable diseases may constitute important grounds of public interest and/or the data subject's vital interests (Recitals 46 and 52). Further, the legal liability of an employer for the health and safety of its employees may necessitate an employer gathering and processing employee personal data to pursue its legitimate interests, subject, of course, to the fundamental rights of the employees. As a result, processing employees' information with respect to their EU-based travel history should have a lawful basis under Article 6, provided that the company makes an appropriately narrow data collection and uses the data solely in a legitimate effort to protect the health of its workforce.

Even where an employer has a lawful basis for processing as described above, the GDPR considers "data concerning health" to be a special category of personal data (often referred to as "sensitive personal data") (Article 9). Processing of sensitive personal data is prohibited unless it is justified on one of several recognized grounds, such as, e.g,, where explicit consent of the data subject is obtained (which again, can be withdrawn, and has heightened requirements to be initially valid). Other grounds allow for processing where it is necessary for (i) carrying out the controller's obligations in the field of employment law, or (ii) reasons of substantial public interest, preventative medicine or public health purposes, (in each case, on the basis of EU or EU Member State law (Article 9)). For EU-based employees, where the employer has a legal duty to protect the health and safety of its employees, processing employees' exposure to and symptoms for COVID-19 should meet this test if the information collection is as narrow as possible and used solely for legitimate health and workforce protection purposes.

The GDPR requires certain disclosures to be made to individuals when their data is collected, including the identity and contact details of the person controlling their data, the purposes for which their information is being processed, who will receive the data and their GDPR rights regarding this information (Article 13). An appropriately drafted email to employees should satisfy such disclosure requirements.

As with any other data transfer outside the EU, if an employee's health or travel-related data is to be transferred from the EU to the United States, such as from an EU-based subsidiary to a US headquarters, unless the "public interest" exception applies as provided for under EU/Member State laws (see above discussion) (Article 49(d)), the US-based employer must (a) subscribe to the US Department of Commerce's Privacy Shield program (Articles 45 and 96), (b) obtain the employee's explicit consent (which can be withdrawn; Section 49(1)(a)); or (c) use binding corporate rules (Article 47) or the EU standard contractual clauses (Article 46(c) & (d)). The cross-border data transfer may also qualify for a special exception if a limited number of data subjects are involved, and

compelling interests are present that are not overridden by the data subjects' rights and freedoms. Many COVID-19-related data collections would qualify for this exception, but, among other conditions, an EU regulator would need to be notified (Article 49 final paragraph).

Once collected, an employee's health and travel-related data is subject to the GDPR's general requirements—including access, corrections, deletion, portability, limited processing, and data security (Articles 15-22 & 32)—and should be protected in accordance with an employer's general GDPR compliance program.

ADA

Pursuant to the Americans with Disabilities Act ("ADA") and similar state and local laws, employers are prohibited from disclosing confidential medical information regarding an employee, which includes the employee's identity. In the case of an employee who has tested positive or otherwise reports exposure to COVID-19, any communications to other employees cannot disclose the employee's name without their consent. This principle was underlined in the Centers for Disease Control and Prevention's ("CDC") recent Interim Guidance for Businesses and Employers, which stated that: "If an employee is confirmed to have COVID-19, employers should inform fellow employees of their possible exposure to COVID-19 in the workplace but maintain confidentiality as required by the [ADA]."[3]

While the affected employee's name should not be disclosed, an employer can identify in a general communication to employees that an individual has tested positive/been exposed to COVID-19 and how the individual believes that he or she may have been exposed. The employer may also reach out to co-workers who may have been in actual contact with the affected individual to advise them, without disclosing the identity of the individual, that a person close to them may have been exposed and that they should closely monitor their medical situation.

[3] *See* CDC's Interim Guidance for Businesses and Employers at https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html.

For further information regarding this memorandum, please contact one of the following:

NEW YORK CITY

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Genevieve Dorment
+1-212-455-3605
genevieve.dorment@stblaw.com

Andrew M. Kofsky
+1-212-455-7437
andrew.kofsky@stblaw.com

Melanie D. Jolson
+1-212-455-3346
melanie.jolson@stblaw.com

Jonathan S. Kaplan
+1-212-455-3028
jonathan.kaplan@stblaw.com

Jacob Lundqvist
+1-212-455-3348
jacob.lundqvist@stblaw.com

PALO ALTO

Harrison J. (Buzz) Frahn
+1-650-251-5065
hfrahn@stblaw.com

Jeffrey E. Ostrow
+1-650-251-5030
jostrow@stblaw.com

WASHINGTON, D.C.

Vanessa K. Burrows
+1-202-636-5891
vanessa.burrows@stblaw.com