How a Crisis Impacts your Privacy Compliance Efforts: COVID-19

The recent novel coronavirus (COVID-19) outbreak is causing significant disruption to the global economy, prompting companies to evaluate and revise their preparedness and response strategies. In the wake of a global health crisis, such as the COVID-19 epidemic, organizations must remain vigilant about their liability exposure and their compliance efforts, including those activities under multi-jurisdictional privacy and data protection regimes.

In response to the epidemic, companies are implementing new protocols to combat the spread of the virus, protect its employees and operations, and prepare for contingencies in the event of an outbreak. Such new protocols often include:

- Collecting travel-related information on employees, contractors, customers, and guests.
- Collecting information on health data from employees, contractors, customers, and guests, such as through a self-declaration on the presence or absence of flu-like symptoms or temperature monitoring.
- Disclosing health-related information to third-parties or public health officials, especially in the event of a suspected or actual outbreak.
- Encouraging personnel to leverage remote working strategies.

With severe penalties for non-compliance in several countries and jurisdictions, companies should ensure that such new protocols remain compliant with applicable privacy and protection laws. This alert focuses on compliance with principal privacy and data protection regimes in the U.S. and the EU, and how companies should consider their security-related strategies during increased sensitive personal data processing and remote work mandates.

1. The EU General Data Protection Regulation (GDPR)

Enacted in May 2018, the GDPR is a sweeping privacy regulation that impacts both private and public organizations operating within the EU. The GDPR contains complex provisions that protect "sensitive personal data," including data about racial or ethnic origin, genetic data, biometric data for the purpose of uniquely identifying a natural person, and, importantly, data concerning health.

The processing of these sensitive data sets is generally prohibited unless an enumerated exemption applies or the data subject (*i.e.*, a natural person) explicitly consents to the processing. In this instance, the GDPR provides an applicable exception to processing health data without consent to protect against a serious cross-border threat to public health and, in particular, to prevent communicable disease. *See* General Data Protection Regulation (GDPR), art. 9(i); GDPR, recital 52.

Carrying heavy penalties for non-compliance, Companies subject to the GDPR should carefully consider their data collection strategies before processing sensitive personal information from employees or customers relating to COVID-19. Even though an exception to the collection of such information may apply, the GDPR still requires companies to observe rigorous requirements of transparency, accountability, data minimization, and prohibitions on unlawful disclosures or cross-border transfer of personal information.

In fact, regulators have already begun issuing statements on such activities. On March 2nd, the Italian Supervisory Authority, Garante, published a statement relating to the processing of personal information to prevent the spread of COVID-19 among employees and others in Italy. The Garante made clear that companies should not collect, in a *systematic* and *generalized* manner, personal data on possible COVID-19 symptoms suffered by their employees or their whereabouts. Rather, the collection of such information should be left to healthcare authorities.

2. California Consumer Privacy Act (CCPA)

With respect to employees in California, companies subject to the CCPA are not subject to comparable comprehensive regulation of employee personal information, in part because the CCPA largely does not apply to employees until at least 2021.

However, companies subject to the CCPA should be mindful that, if they collect personal information (broadly defined to include personal identifiers as well as medical, biometric, and thermal information) from California resident consumers (*i.e.*, clients or customers), they will need to observe notice and transparency requirements, as well as accommodate consumer rights that the CCPA provides to California residents. Similar to the GDPR, the CCPA carries significant penalties for non-compliance and – in the event of a data breach – exposure to individual or class-wide private actions. As a result, companies should carefully consider their proposed strategies before processing sensitive personal data from consumers relating to COVID-19.

3. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

For those companies or organizations subject to HIPAA (*i.e.*, organizations that are covered entities or business associates that collect or process protected health information), the HIPAA Privacy Rule and related regulations protect the privacy of such personal health information. The Rule, however, is balanced to ensure that appropriate uses and disclosures of the information still may be made when necessary to treat a patient, to protect the nation's public health, and for other critical purposes.

Critically, HIPAA permits covered entities to disclose protected health information, without authorization, to public health authorities in order to prevent or control disease. Absent mandatory reporting requirements, information that an employee or customer has been exposed to or has received a confirmed COVID-19 diagnosis should be shared only on a need-to-know basis and documented separately. Organizations should not – beyond the team authorized to address the diagnosis disclosure – provide personal information that, in the aggregate, could identify the affected individual.

Likewise, certain states have health privacy laws that extend beyond HIPAA's scope and requirements. For example, California's Confidentiality of Medical Information Act (CMIA) requires all entities subject to the Act (including employers not covered by HIPAA) that receive medical information (defined broadly to include individually identifiable health information about a patient's medical history, mental or physical condition, or treatment) to establish policies to maintain the confidentiality of such information. The CMIA also prohibits employers from using or disclosing such medical information without a signed authorization from the employee except as required by law.

4. Cyber and Physical Security Efforts om the Wake of a Health Crisis

Finally, in addition to good security hygiene generally, the protection of information is a requirement under various privacy regimes. Criminals are capitalizing on the crisis, and – in an effort to protect personnel – companies are encouraging increased remote work strategies, which can carry significant security vulnerabilities.

With the public's intense interest in COVID-19, "phishing" scams are on the rise and criminals are attempting to leverage false information about the coronavirus to lure email recipients into following nefarious links. Successful phishing attacks can release malware onto corporate systems or trick employees into providing login credentials or other sensitive information to unauthorized third parties. The campaigns are so prevalent that the World Health Organization (WHO) released a statement warning of criminals disguised as the WHO.

In anticipation of continuing malware campaigns and other cyber-vulnerabilities associated with increased remote working strategies, companies should encourage employees to remain vigilant when reviewing correspondence and to engage only with official information sources. In addition, companies should consider the following proactive initiatives:

- Conduct workplace or online training about COVID-19-related phishing and malware campaigns.
- Reinforce remote work policies, including the use of virtual private networks and the use of company-issued devices (rather than the use of personal devices).
- Ensure that mobile devices are equipped with mobile device management software.
- Review the company's incident response plan, including plans to quickly (i) investigate the nature and scope of any attack, (ii) ensure that any attackers are not still present in the systems, (iii) determine whether notification is required under applicable state law to individuals and state agencies, and (iv) help employees whose personal information may have been compromised.
- Review the company's business continuity plans in the event of a disruption from a critical service provider or a successful attack, such as a DDoS or ransomware attack.
- Ensure that the company infrastructure protections are up-to-date, including all patch requirements, properly-configured firewalls, updated white and black lists, and ensuring that different tools and technologies are in-place, such as DDoS mitigation tools.
- Ensure that the company has the proper bandwidth to accommodate increased remote working solutions.

Companies should remain vigilant and encourage good security hygiene from all employees. It is important to remember that all companies are different, and varying controls and procedures may be appropriate depending on the size and complexity of the company, as well as the sensitivity of the information maintained by the company.

If you have any questions regarding these issues, questions or concerns about compliance with privacy requirements, or how your organization can improve its security posture, please contact Matthew R. Baker or any member of Baker Botts' Privacy and Data Security team.