BARNES & THORNBURG LLP

ALERTS

COVID-19 And Global Data Protection

March 18, 2020

As the world around us struggles to contain the spread of COVID-19, over the last few weeks public and private institutions have dramatically increased the rate of activities that may involve the processing of large quantities of personal data – with the aim of protecting public health and the welfare of society at large.

With increased processing of frequently sensitive personal medical information comes the escalating risk of violating individuals' rights as warranted by various data protection statutes around the world, including the GDPR, HIPAA and the CCPA. These global data protection and privacy laws will still apply, even in these uncertain times.

This alert will address some of the concerns related to privacy and data protection, while balancing entities' legitimate interests in protecting public health on one side and individuals' rights to privacy on the other.

The EU General Data Protection Regulation (GDPR)

Nearly all European Data Protection Authorities (DPAs) – which monitor companies' compliance with applicable laws (particularly, the GDPR) daily – are in agreement that although "data protection laws do not stand in the way of the provision of healthcare and the management of public health issues, important considerations with respect to handling of personal data and particularly, sensitive medical data," should be taken under advisement.

Various DPAs advise that while data controllers may take measures that impair the privacy of individuals, they may not go beyond reasonable management of a crisis in a manner that impedes the "fundamental human right" an individual has to the protection of their personal data. For

RELATED PEOPLE

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

RELATED PRACTICE AREAS

COVID-19 Resources
Data Security and Privacy

example, data controllers are not likely permitted to engage in the systematic collection of mandatory readings of body temperature or collection of compulsory health questionnaires.

The management of the COVID-19 crisis also does not excuse data controllers from the applicability of other GDPR-related fundamentals. While most entities may presumably conduct their COVID-19-related processing "lawfully," pursuant to one or more of the legal bases provided by GDPR, they must limit such processing to only what is necessary and proportionate while maintaining confidentiality.

Additionally, data controllers should be cautious to only collect the minimum necessary amounts of personal data to accomplish tasks at hand and do so in a manner that ensures security and confidentiality of the data, particularly where medical data is concerned. For example, in a hypothetical scenario involving a U.S. employer and its Europe-based employees, the employer may not reveal the identity of impacted individuals to any third parties or to their colleagues without a clear justification and consideration of GDPR requirements.

The U.S. Health Insurance Portability and Accountability Act (HIPAA)

Even though the HIPAA rules continue to apply to HIPAA -covered entities, when public health emergencies are declared, the secretary of Health and Human Services (HHS) may choose to waive certain sanctions and penalties for noncompliance with specific provisions of the HIPAA Privacy Rule. Most recently, on March 17, 2020, the HHS secretary of has exercised its enforcement discretion, announcing that the office "will waive potential penalties for HIPAA violations against health care providers that serve patients through everyday communications technologies during the COVID-19 nationwide public health emergency."

This unprecedented exercise of discretion applies to widely available communication apps, such as FaceTime or Skype, when used in good faith for any telehealth treatment or diagnostic purposes, regardless of whether the telehealth service is directly related to COVID-19. The Office for Civil Rights (OCR) is expected to provide further guidance explaining how covered healthcare providers can use remote video communication products and offer telehealth to patients responsibly.

Similarly, effective March 15, 2020, the HHS announced a limited HIPAA waiver covering the following provisions of the HIPAA Privacy Rule:

- Requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care
- Requirement to honor a request to opt out of the facility directory
- Requirement to distribute a notice of privacy practices
- Patient's right to request privacy restrictions
- Patient's right to request confidential communications

Notably, the HIPAA waiver only applies in areas covered in a public health

emergency, for hospitals that have implemented their disaster protocol, and for a period of 72 hours from the time that the disaster protocol is implemented. When the declaration terminates, hospitals must then comply with HIPAA Privacy Rule requirements for patients still under their care, even if 72 hours have not elapsed.

The California Consumer Privacy Act (CCPA)

The **California Consumer Privacy Act** (CCPA), which went into effect Jan. 1, 2020, and applies to the personal information of California consumers, notably includes a carve-out for HIPAA-covered entities and business associates. CCPA generally does not apply to HIPAA-regulated protected health information (PHI), such as that likely to be collected during public health emergencies. However, HIPAA-covered businesses must still exercise caution and provide appropriate privacy disclosures when collecting non-HIPAA regulated PHI or other information that may be classified as "personal information" of California residents, which clearly would still be subject to requirements of the CCPA.

Entities should also continue best practices for data collection, use and sharing any time sensitive or personal information of individuals is being processed.

Summary

The data protection frameworks applicable to U.S. entities and organizations include limited exemptions from various privacy-related obligations that are intended to be triggered during public health emergencies, such as the current COVID-19 pandemic. That said, entities should remain vigilant and collect or otherwise process only necessary and proportionate personal information, while maintaining the confidentiality and security of such data.

For more information, contact the Barnes & Thornburg attorney with whom you work or Brian McGinnis at 317-231-6437 or brian.mcginnis@btlaw.com; or Michael Baumert at 312-214-4570 or michael.baumert@btlaw.com, or Rocky Cislak at 317-29-3144 or rocky.cislak@blaw.com.