MILLER CANFIELD

COVID-19: Data Privacy Compliance

March 17, 2020

By Justyna Regan

Managing the COVID-19 outbreak requires adopting measures that have never been seen before. Such measures, aimed at monitoring how the virus spreads, inevitably require processing "personal data," including health information about individuals who may have been exposed or infected with the virus. Below we highlight some data privacy considerations that address key issues to keep in mind.

HIPAA Employee Personal Data

Last month, the U.S. Department of Health and Human Services published the bulletin "*HIPAA Privacy and Novel Coronavirus,*" explaining certain applicable HIPAA privacy rules in light of the COVID-19 pandemic. These rules authorize covered entities subject to HIPAA, which include health plans, clearinghouses, and certain health care providers, to disclose protected health information ("PHI") without a patient's authorization, as necessary to treat that patient or any other patient. HIPAA also allows making PHI available to a public health authority, a foreign governmental agency that is acting in collaboration with a public health authority or a person who may have been exposed to or is otherwise at risk for contracting COVID-19. HIPAA also permits health care providers to share a patient's PHI as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public. However, all disclosures of PHI under HIPAA must be limited to the minimum extent necessary to accomplish the purpose.

For more, see: **https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf**.

Employee Personal Data

With respect to employment personal data, the U.S. Equal Employment Opportunity Commission (EEOC) **posted guidance** on its website that can help employers implement strategies to navigate the impact of coronavirus in the workplace. The guidance dates back to 2009 as a response to the H1N1 outbreak, which is instructive to employers in dealing with COVID-19 workplace situations. Additional information was added the morning of March 17, 2020.

The EEOC has clarified that during the COVID-19 pandemic, employers may take measures that are job-related and consistent with business necessity, which could impact employees' privacy. Employers may ask employees who report feeling ill at work or call in sick if they are experiencing COVID-19-like symptoms, and if such cases are confirmed, an employee who became ill with symptoms of COVID-19 can be required to leave the workplace. Please also note that according to the guidance, the employer is authorized to measure employees' body temperature. Upon return to work, the employer may require employees to present doctor's notes certifying their fitness for duty. Nonetheless, employers must always keep employees' medical and health-related information and records confidential.

For more, see: **https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.**

GDPR

For U.S. businesses required to comply with the European Union's **General Data Protection Regulation** ("GDPR"), the GDPR lists several narrowly interpreted exceptions, which exclude application of the general rules on data processing, including:

- Processing personal data if such processing "*is necessary in order to protect the vital interests of the data subject or of another natural person*", which is further explained as "*processing [that] may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.*" In other words, even if the data subject did not grant his/her consent, processing may be carried on if it qualifies to the aforementioned exception;
- Processing special categories of data, e.g. data concerning health (which includes any information on a disease or disease risk), is generally prohibited, unless "*processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices,*" "*processing is necessary for the purposes of preventive or occupational medicine,*" or "*processing is necessary for reasons of substantial public interest.*" The preamble further clarifies that such processing shall be allowed where it is in the public interest to do so, in particular processing in the field of social protection law including prevention or control of communicable diseases and other serious threats to health;
- Right to be forgotten is excluded to the extent that processing is necessary "*for reasons of public interest in the area of public health.*"

CCPA

Please note that the California Consumer Privacy Act of 2018 ("CCPA") excludes from its scope health information and health care providers covered under the California Confidentiality of Medical Information Act and HIPAA.

This is part of a series of our **COVID-19 alerts** providing clients with practical advice on measures they can take to navigate through these troubled times. Please contact the authors or your Miller Canfield attorney with further questions.

This information is based on the facts and guidance available at the time of publication, and may be subject to change.