Benesch

April 23, 2020

BIWEEKLY ALERT

From Benesch's **Data Privacy Defense & Response Team**

COVID-19's Impact on Data Privacy Laws and Regulations

There is likely no question that COVID-19 is having an impact on your business. But have you considered the way the pandemic is impacting the privacy laws that guide your business practices? Here are a few examples of the impact COVID-19 has had on data privacy laws:

- **A New Era of Relaxed HIPAA Requirements:** The Office of Civil Rights (OCR) has issued guidance on permitting increased "flexibility" under HIPAA. OCR has indicated that it will be exercising its enforcement discretion to not impose penalties for HIPAA violations against healthcare providers in connection with their good-faith provision of telehealth services using communication technologies during the COVID-19 nationwide public health emergency. OCR has also announced that it will not penalize hospitals or their business associations for disclosing COVID-19-related PHI, with the goal of supporting public health authorities, such as the CDC, CMS, and local health departments, in gaining access to COVID-19-related data. OCR has also issued guidance relaxing HIPAA protections related to PHI disclosed to first responders who need to determine whether they must take extra precautions when dealing with specific patients. These new, more flexible HIPAA guidelines stand in contrast to the normally rigid privacy regime most businesses are used to.
- **The New York SHIELD Act Creates New Liability in Uncertain Times:** The pandemic obligated many businesses to quickly adapt their IT infrastructures to accommodate company-wide work-from-home measures. Such rapid-fire changes inevitably strained businesses' IT resources, which left them vulnerable to cybercriminals and caused a spike in attacks. In the meantime, the New York SHIELD Act went quietly into effect on March 21, 2020, significantly expanding businesses' liability risks and requiring them to implement more robust data security programs to further protect the personal data of New York residents. The SHIELD Act requires businesses to include specific elements in their data security plans, including designating an employee to oversee cybersecurity operations,

(continued)

Please note that this information is current as of the date of this client bulletin, based on the available data. However, because COVID-19's status and updates related to the same are ongoing, we recommend real-time review of guidance distributed by CDC and local officials.

For more information, please contact one of the following members of Benesch's Data Privacy Defense & Response Team:

MICHAEL D. STOVSKY
Partner and Chair, Innovations, Information Technology & Intellectual Property (3iP) Practice Group; Chair, Data Security & Privacy Team; Chair, Blockchain & Smart Contracts Team
T: 216.363.4626 | mstovsky@beneschlaw.com

J. ERIK CONNOLLY
Partner and Vice Chair, Litigation Practice Group; Co-Chair, Securities Litigation Practice Group
T: 312.624.6348 | econnolly@beneschlaw.com

ALISON K. EVANS
Associate, 3iP Practice Group; Data Security & Privacy Team
T: 216.363.4168 | aevans@beneschlaw.com

WHITNEY M. JOHNSON
Associate, Litigation Practice Group
T: 628.600.2239 | wjohnson@beneschlaw.com

KATE WATSON MOSS
Associate, Litigation Practice Group
T: 312.624.6329 | kwatsonmoss@beneschlaw.com

COVID-19's Impact on Data Privacy Laws and Regulations

(continued from previous page)

providing employees with regular training on data security issues, and selecting service providers that are employing equally strong security safeguards. The statute also requires timely disposal of personal information that is no longer necessary for business purposes, and expands the New York attorney general's authority to enforce against failure to timely report a security incident in accordance with New York's breach notification law and failure to comply with the new data security standards.

- **CCPA Enforcement Looms:** The California Attorney General's Office has yet to issue final guidance on the California Consumer Privacy Act (CCPA), but that's no obstacle for enforcement of the state's groundbreaking data privacy law. Despite recent lobbying efforts from business owners who now find themselves and their workforces living in a coronavirus world—and who would prefer to focus their time and energy on COVID-19 relief efforts and making sure that they stay in business—Attorney General Xavier Becerra is on track to begin enforcement efforts starting July 1. If understanding the impacts of CCPA was a challenge before, then the fallout from COVID-19 can best be understood as muddying the waters as to the risks, uncertainties, and impacts of the new law. Indeed, Zoom, Facebook, and LinkedIn are already facing consumer class action lawsuits with COVID-19-based CCPA claims. What's next?

Now is the time to take action to protect your business, customers, and employees. We invite you to participate in a complimentary 30-minute call with Benesch's data protection specialists. Benesch would be happy to provide you with our insight and guidance on data protection best practices and litigation avoidance strategies. We look forward to working with you to keep your data safe and secure.