As they work to combat the surging COVID-19 virus, healthcare providers recently were reminded by legislators and regulators of the importance of data security and privacy protections.

On the data security front, U.S. Senators Richard Blumenthal, Tom Cotton, David Perdue, and Mark Warner recently wrote to the Director of the U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Agency (“CISA”) and the commanding general of the U.S. Cyber Command to express their “profound concerns” that healthcare providers are “facing an unprecedented and perilous campaign of sophisticated hacking operations from state and criminal actors amid the coronavirus pandemic,” which “pose an alarming risk of disrupting or undermining our public health response at this time of crisis.” The Senators urged CISA and the Cyber Command to issue guidance and provide technical resources to deter these threats.
Beyond their general call for action, the Senators offered specific measures CISA and the Cyber Command should adopt to protect healthcare providers’ data security:

1. Provide private and public cyber threat intelligence information, such as indicators of compromise (IOCs), on attacks against the healthcare, public health, and research sectors, including malware and ransomware.
2. Coordinate with the Department of Health and Human Services, the Federal Trade Commission, and the Federal Bureau of Investigation on efforts to increase public awareness on cyberespionage, cybercrime, and disinformation targeting employees and consumers, especially as increased telework poses new risks to companies.
3. Provide threat assessments, resources, and additional guidance to the National Guard Bureau to ensure that personnel supporting state public health departments and other local emergency management agencies are prepared to defend critical infrastructure from cybersecurity breaches.
4. Convene and consult partners in the healthcare, public health, and research sectors, including its government and private healthcare councils, on what resources and information are needed to reinforce efforts to defend healthcare IT systems, such as vulnerability detection tools and threat hunting.
5. Consider issuing public statements regarding hacking operations and disinformation related to the coronavirus for public awareness and to put adversaries on notice, similar to the joint statement on election inference issued on March 2nd.
6. Evaluate further necessary action to defend forward in order to detect and deter attempts to intrude, exploit, and interfere with the healthcare, public health, and research sectors.

On the heels of this call for action on data security, the Office for Civil Rights (“OCR”) at the U.S Department of Health and Human Services issued additional guidance reminding covered health care providers that the HIPAA Privacy Rule does not permit them to give media and film crews access to facilities where patients’ protected health information will be accessible without the patients’ prior authorization. In this guidance, the OCR reiterated that “it is not sufficient for a covered health care provider to require the media to mask patients’ identities when airing recorded video (such as by blurring, pixelation, or voice alteration), after the fact. Prior, express authorization from the patient is always required.” While this guidance does not break new ground, it serves as a timely reminder as newscasts focus daily on the efforts of healthcare providers to treat COVID-19 patients.

These are difficult times for healthcare providers, but even as they tackle the clinical demands of the COVID-19 pandemic, the developments discussed above demonstrate the importance of continuing to be vigilant in the enforcement of data security and privacy policies.

Jackson Lewis P.C. © 2020