ROB BONTA
Attorney General

State of California
DEPARTMENT OF JUSTICE

1300 "I" Street
Sacramento, CA 95814-2919

Public: (916) 445-9555

August 24, 2021

BULLETIN: Obligation to Proactively Reduce Vulnerabilities to Ransomware Attacks and Requirements Regarding Health Data Breach Reporting

The privacy and security of health data is essential and protects the public from losses that could result from the fraudulent use of consumers' personal information obtained from a breach of health data. As such, providers of healthcare have a continuing obligation to comply with the requirements of state and federal health data privacy laws, especially those regarding health data breach reporting.

The California Department of Justice, Office of the Attorney General (OAG) is committed to enforcing consumer protection and health privacy laws to protect the health data of Californians. The healthcare sector has been a main target of cyberattacks. Across the nation, cyberattacks on the healthcare sector has interrupted service delivery and patient care, and eroded patient trust. Data breaches, particularly when they involve sensitive information such as Social Security numbers and health records, threaten the privacy, security, and economic wellbeing of consumers. The effects of a health data breach on consumers outlast the initial breach. Timely breach notification helps affected consumers mitigate the potential losses that could result from the fraudulent use of their personal information obtained from a breach of health data. Therefore, it is important for providers of healthcare to be proactive and vigilant about reducing their risk for ransomware attacks and to meet their health data breach notification obligations to protect the public.

State and federal health data privacy frameworks, like the Confidentiality of Medical Information Act (CMIA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), obligate healthcare entities and organizations that deal in health data to establish appropriate procedures to ensure the confidentiality of health-related information, including security measures that can help prevent the introduction of malware, including ransomware, to protect consumers' healthcare-related information from unauthorized use and disclosure.[1] As

[1] Unless a federal action is pending, the California Attorney General has authority to bring civil actions on behalf of California residents for violations of the HIPAA, as amended by the Health Information Technology for Clinical and Economic Health (HITECH) Act. 42 U.S.C. §1320d- 5(d). Federal law requires both covered entities and business associates to provide a notification of a breach of protected health information to affected individuals, the Secretary of the U.S. Department of Health and Human Services, and in certain circumstances, to the media. 45 C.F.R. §§ 164.400-414. In addition, business associates must notify covered entities if a breach occurs at or by the business associate. *Id.*

such, healthcare entities should, at a minimum, take the following preventive measures to protect its data systems from ransomware attacks:

- keep all operating systems and software housing health data current with the latest security patches;
- install and maintain virus protection software;
- provide regular data security training for staff members that includes education on not clicking on suspicious web links and guarding against phishing emails;
- restrict users from downloading, installing, and running unapproved software; and
- maintain and regularly test a data backup and recovery plan for all critical information to limit the impact of data or system loss in the event of a data security incident.

In addition, healthcare entities should also continue to monitor health data security advisories from government agencies, like the OAG, and also federal agencies like the U.S. Department of Health and Human Services, Office for Civil Rights, the Cybersecurity & Infrastructure Security Agency, the National Institute of Standards and Technology, the Federal Bureau of Investigation, the U.S. Department of Justice, and the U.S. Department of Homeland Security. Consumers and businesses may also refer to the federal government's newly launched website, https://www.cisa.gov/stopransomware, for additional information and resources for private and public organizations mitigate their ransomware risk.

State and federal privacy laws also require healthcare entities, and their vendors who handle health-related data on the healthcare entity's behalf, to protect the privacy and security of the health-related data in their custody. When these entities and their vendors suffer a breach, they must comply with their breach notification obligations. California has comparable breach notification requirements as federal law. Under California Civil Code section 1798.82, any person or business that conducts business in California that owns or licenses "computerized data" that includes personal information must notify the OAG if the data of 500 or more residents of California was, or is reasonably believed to have been, acquired by an unauthorized party as the result of a breach of security. Therefore, entities that have suffered a data breach, including a health data breach, affecting 500 or more California residents must submit a breach report to the OAG.[2]

The OAG will continue our work to protect the privacy and security of consumer health data. Healthcare providers and their vendors should prioritize safeguarding the privacy and security of consumer healthcare data. This includes proactively implementing data security measures and submitting timely breach reports in the event of a security incident to the OAG when a breach impacts the health data of 500 or more California residents. At the same time, the

[2] *California Department of Justice, Office of the Attorney General Data Security Breach Reporting*, https://oag.ca.gov/privacy/databreach/reporting.

OAG is committed to maintaining open lines of communication with healthcare providers and their vendors to ensure continued compliance with state and federal requirements.