## California AG Appendix

On December 9, 2019, Overlake learned of an email compromise, or phishing incident, that resulted in the unauthorized access to employee email accounts between December 6, 2019 and December 9, 2019. Overlake immediately secured the accounts and began an investigation, and a cyber security firm was engaged to assist. Through its investigation, Overlake determined that an unauthorized party may have been able to access patient information contained in the email accounts. Overlake determined that these emails may have included information belonging to 1,087 California residents, including some or all of the following data elements: demographic information, health insurance information, and limited clinical information.

On February 4, 2020, Overlake mailed notification letters in substantially the same form as enclosed, in compliance with the Health Insurance Portability and Accountability Act of 1996, as amended, and its Regulations including 45 C.F.R. § 164.404.* It has also established a dedicated call center where affected individuals may obtain more information regarding the incident.

To help prevent something like this from happening again, Overlake has implemented additional security measures to protect its systems, including resetting passwords for all compromised employee accounts to prevent further unauthorized access; enhancing the already mandatory education for employees to help them better recognize and avoid phishing emails; enhancing the technology in use to identify and block suspicious external emails; and implementing multi-factor authentication, which requires staff to go through multiple steps to verify their identity in order to access systems.

*This report does not waive Overlake's objection that California lacks personal jurisdiction over this matter.