Dear Medical Professionals:

This message is distributed by the State of California Alert Health Network and is intended to provide general cyber security tips, guidance, and advisories to help our medical sector partners. Cyber threats have been increasing *in response to this pandemic*, targeting all sectors, and the medical sector is not excluded.

The State of California would like to remind our medical sector partners to remain vigilant for scams *and data theft* related to Coronavirus Disease 2019 (COVID-19). Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.

When it pertains to leveraging any technology or communications, we encourage our medical industry partners to take the following precautions:

- Avoid clicking on links in unsolicited emails and be wary of email attachments. See Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams for more information.
- Use trusted legitimate sources such as, government websites for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information.

For additional information we encourage your Information Security contacts to leverage the following:

- The California Cyber Security Integration Center (Cal-CSIC) cyber advisories and threat information on online schemes related to COVID-19. For continued information, register your organization Information Security contact online at https://calcsic.org.
- For Information technology and cyber security teams, email the Cal-CSIC (calcsic@caloes.ca.gov) to learn more about threat indicators and connecting to the California Automated Indicator Exchange. ~~at~~
- If *a* cyber-related issue~~d~~ occurs please report the incident~~s~~ to the Cal-CSIC at (833) REPORT-1 or calcsic@caloes.ca.gov.

The Cal-CSIC is a multi-agency integration center comprised of intelligence and cybersecurity specialists from multiple agencies, including the California Governor's Office of Emergency Services (Cal OES), the California Department of Technology (CDT) and the State's Chief Information Security Office (CISO), the California Highway Patrol's Computer Crimes Investigation Unit (CCIU), the California Military Department (CMD) aka California National Guard, as well as representatives from DHS CISA and the Sacramento Field Office of the FBI. The Cal-CSIC serves as the central hub of the State's cybersecurity activities, including strategic policy, cyber threat analysis, risk assessment, and alert; information sharing between Federal, State, Local, Tribal, academia, critical infrastructure, and public sector entities.