STATE OF WASHINGTON
DEPARTMENT OF SOCIAL AND HEALTH SERVICES
Aging and Long-Term Support Administration
PO Box 45600, Olympia, WA 98504-5600

February 6, 2017

ALTSA: ICF/IID #2017-001
S&C: 17-17-ALL: RECOMMENDATIONS REGARDING CYBER SECURITY

Dear ICF/IID Superintendents and Administrators:

The Centers for Medicare & Medicaid Services (CMS) is reminding providers and suppliers to keep current with best practices regarding mitigation of cyber security attacks. We have outlined resources to assist facilities in their reviews of their cyber security and IT programs.

The Cybersecurity Act of 2015, section 405(b) required the Department of Health and Human Services (HHS) to develop a report on the preparedness of HHS and health care industry stakeholders in responding to cybersecurity threats. This report is known as the U.S. HHS Preparedness Report and outlines the HHS components responsibilities for cyber security. However, the report does not outline mechanisms for States and facilities regarding procedures to take to protect themselves from adverse cyber events.

CMS recommends that facility leadership review current policies and procedures to ensure adequate plans are in place in the event of an attack. For instance, most IT Directors and policies within facilities require systems to be shut down, and specific timelines to notify appropriate State and Federal agencies and State Health Departments.

Additional information and the S&C memo can be accessed via the CMS website at: https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-17-17.pdf

Thank you for your continued commitment to the health and safety of nursing home residents. If you have any questions, please contact your local RCS Field Manager.

Sincerely,

Candace Goehring

Candace Goehring, Director
Residential Care Services

"Transforming Lives"