TEXAS
Health and Human Services

Texas Health and Human Services Commission

Cecile Erwin Young
Executive Commissioner

Date: February 24, 2021

To: Adult Foster Care Providers
Community Attendant Services Providers
Community Living Assistance and Support Services Providers
Client Managed Personal Attendant Services Providers
Day Activity & Health Services Providers
Deaf Blind with Multiple Disabilities Providers
Emergency Response Services Providers
Family Care Providers
Financial Management Services Agencies
Home and Community-based Services Providers
Home and Community-based Services-Adult Mental Health Providers
Home Delivered Meals Providers
Hospice Providers
Intermediate Care Facilities for Individuals with an Intellectual Disability or Related Condition
Local Intellectual and Developmental Disability Authorities
Primary Home Care Providers
Program of All-inclusive Care for the Elderly Providers
Special Services to Persons with Disabilities Providers
Relocation Services Providers
Residential Care Providers
Texas Home Living Providers
Transition Assistance Services Providers
Youth Empowerment Services Providers

Subject: Information Letter No. 2021-09 (Replaces IL 2012-86)
Handling of Sensitive Personal Information and Breach Notification

This letter provides updated information regarding responsibilities and requirements relating to protecting sensitive personal information received from the Health and Human Services Commission (HHSC) and notifying HHSC of a breach of sensitive personal information. This information letter (IL) replaces IL2012-86, Handling of Sensitive Personal Information and Breach Notification.

As part of its contract with HHSC, a provider or agency may receive or create sensitive personal information, as defined in section 521.002 of the Business and Commerce Code. The provider or agency must use appropriate safeguards to protect this sensitive personal information from unauthorized disclosure or acquisition. These safeguards must include maintaining the sensitive personal information in a form that is unusable, unreadable, or indecipherable to unauthorized persons. The provider or agency may consult the "Guidance to Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals" issued by the U.S. Department of Health and Human Services to determine ways to meet this standard.

Upon discovery, the provider or agency must notify HHSC of any confirmed or suspected unauthorized acquisition, access, use or disclosure of sensitive personal information related to its contract with HHSC, including any breach of system security, as defined in section 521.053 of the Business and Commerce Code. The provider or agency must submit Form 0402 Potential Privacy/Security Incident, to HHSC as soon as possible but no later than 10 business days after discovering the unauthorized acquisition, access, use or disclosure. The provider or agency must include on the form the identity of each individual whose sensitive personal information has been or is reasonably believed to have been compromised.

The provider or agency must disclose the unauthorized acquisition, access, use or disclosure to each individual whose sensitive personal information has been or is reasonably believed to have been compromised or pay the expenses associated with HHSC providing the notification if:

- The provider or agency experiences a breach of system security involving information owned by HHSC for which disclosure is required under section 521.053 of the Business and Commerce Code; or
- The provider or agency experiences a breach of unsecured protected health information, as defined in 45 CFR §164.402, and HHSC becomes responsible for providing the notification required by 45 CFR §164.404.

HHSC may, at its discretion, waive the provider's or agency's payment of expenses associated with HHSC providing the notification. Notification must be done without unreasonable delay and by, at most, the 60th day following the discovery date of

the incident. Exception may be made at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.

To report an unauthorized disclosure or acquisition of sensitive personal information, email a completed Form 0402 Potential Privacy/Security Incident to the HHS Privacy Division at privacy@hhsc.state.tx.us.

For questions regarding the content of this letter please contact HHS Chief Privacy Officer, Sarah Morrow at sarah.morrow@hhs.texas.gov or the HHS Privacy Division at 877-378-9869.

Sincerely,

[signature on file]

Michelle Erwin
Deputy Associate Commissioner
Policy and Program
HHSC Medicaid and CHIP Services