

**Health Insurance Portability and Accountability Act (HIPAA) and Privacy Laws**

The Health Insurance Portability and Accountability Act (HIPAA) privacy rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the privacy rule is balanced so that it permits the disclosure of personal health information (PHI) needed for patient care and other important purposes. Texas state laws and legislation strengthen the protection to include an individual's sensitive personal information (SPI).

As a covered entity, DADS contract providers are mandated to follow the HIPAA and privacy laws, as well as state legislation. Legislation requires that a covered entity:

* Ensures the security and safeguard of protected health information (PHI) and sensitive personal information (SPI).
* Provides HIPAA and privacy training to employees, contract employees and volunteers.
* Requires an employee, contract employee, volunteer or manager to report a potential violation incident to the covered entity's management or Privacy Office.
* Requires the covered entity to assess the validity of an incident, and provide notification if required.
* Reports HIPAA violations and findings to the federal secretary of Health and Human Services (HHS), as required.

## What is an Incident?

An incident is an event, which may result or appear to have resulted, in accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of confidential information. An incident may result in the possession of unauthorized knowledge, the wrongful disclosure of information, embarrassment to the agency, the unauthorized alteration or destruction of information or systems, or violation of federal or state laws or regulations or agency business requirements.

## Contacting with DADS

As part of its contract with the Texas Department of Aging and Disability Services (DADS), a provider or agency may receive or create sensitive personal information, as Section 521.002 of the Business and Commerce Code defines that phrase. The provider or agency must use appropriate safeguards to protect this sensitive personal information from unauthorized 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"](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html), issued by the U.S. Department of Health and Human Services, to determine ways to meet this standard.

## Reporting Incidents

The provider or agency must notify DADS of any unauthorized acquisition of sensitive personal information related to its contract with DADS, including any breach of system security, as section 521.053 of the Business and Commerce Code defines that phrase.

The provider or agency must submit [Form 0400, Privacy Incident Report](https://www.dads.state.tx.us/forms/0400/index.htm), to DADS Privacy Office as soon as possible but no later than 10 business days after discovering the unauthorized acquisition. 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 involved in the unauthorized acquisition.

To report an unauthorized acquisition of sensitive personal information, email a completed Form 0400 to DADS HIPAA Privacy Office at Privacy.Office@dads.state.tx.us.

Additional information regarding HIPAA is available at the [U.S. Department of Health and Human Services, Office of Civil Rights website](http://www.hhs.gov/ocr/privacy/index.html).

## Contact Us

If you have questions regarding this webpage or Form 0400, Privacy Incident Report, contact DADS Executive and Staff Operations, Administrative Management Services, Privacy Office, at 1-877-379-7410 or by email at Privacy.Office@dads.state.tx.us.