TEXAS
Health and Human
Services Commission

DATA USE AGREEMENT

DUA – WHAT IS IN IT?

Article 1 – Purpose: Applicability: Order of Precedence

When an HHS contractor creates, receives, maintains, uses, discloses or accesses HHS confidential information, a DUA describes the privacy, security and breach notification requirements the contractor must adhere to so that HHS confidential information is protected.

The DUA takes precedence if there are conflicting terms in the Base Contract.

Article 2 – Definitions

The definitions in the DUA come from the statutes and regulations that apply to particular types of confidential information.

Confidential Information includes the following:

- Client information:
  - --Protected Health Information
  - --Sensitive Personal Information
  - --Personally Identifiable Information
  - Federal Tax Information
- Social Security Administration Data
- Privileged work product
- Information designated confidential under PIA

Article 3 – Contractor's Duties Regarding Confidential Information

Contractor must

- Limit access to CI to only Authorized Users for an Authorized Purpose (the services that HHS has hired the contractor to perform)
- Train its Workforce on privacy and security
- Sanction its Workforce who violate the DUA
- Not re-identify de-identified CI
- Be responsible for its subcontractors and have them sign the Subcontractor Attachment to the DUA
- Maintain privacy and security policies and procedures and accountings of disclosures of, and amendments to, PHI.
- Return or Destroy CI upon termination of DUA at HHS' election

Article 3 (Cont.)

- Provide a Security and Privacy Inquiry (SPI) or System Security Plan to HHS that documents contractor's security controls and identifies security risks
- Establish and implement administrative, procedural, technical and physical safeguards that protect CI
- Identify a Privacy Official and an Information Security Official to be responsible for the implementation of the DUA and contact with HHS
- Maintain a list of Authorized Users
- Respond to HHS requests for information and cooperate with investigations and audits
- Securely transmit CI (may include encryption)
- Comply with applicable laws, regulations, security controls and policies

Article 4 – Breach Notice, Reporting and Correction

The DUA has STRICT initial breach notice requirements.

Within One Hour
(if the information came from a federal system of records):

- Federal Tax Information
- Medicaid client information
- Social Security Administration Data

Within 24 Hours:

- Protected Health Information
- Sensitive Personal Information
- Other non-public information

Article 4 (Cont.)

Contractor must report the breach to HHS at privacy@hhsc.state.tx.us

and report to your HHS contract manager.

Article 4 (Cont.)

Contractor must

- Investigate the breach
- Notify HHS of
  - date of breach
  - date it was discovered
  - description of events
  - type and amount of confidential information
  - identity and number of affected individuals
  - risk assessment
  - steps to protect individuals from harm
  - steps to prevent recurrence
  - law enforcement involvement

Article 4 (Cont.)

Contractor must

- Keep HHS updated and participate on incident response team
- Take corrective action (mitigate) the breach
- Cooperate with HHS
- Timely notify affected individuals (if required)
- Obtain HHS approval for communications
- Respond to regulatory authorities
- Deliver final assessment and mitigation report to HHS

Article 5 – Scope of Work

This section connects the DUA to the base contract.

The Scope of Work identifies the Authorized Purpose (the contractor services) for which contractor is permitted to access Confidential Information.

Article 6 – General Terms

- HHS is the owner of the CI with a few exceptions, e.g., local mental health authorities
- HHS will not ask contractor to do anything with CI contrary to law
- HHS can inspect or audit contractor facilities, systems, books and records
- HHS may terminate the DUA (and Base Contract) for breach of the DUA (obligation to protect CI survives termination)
- HHS may seek other relief for breach of the DUA including asking for a corrective action plan
- Texas law governs

Article 6 (Cont.)

- Contractor will indemnify HHS for any losses arising from contractor's acts or omissions related to the DUA
- Contractor may be asked to carry insurance sufficient to cover losses under the DUA if high risk
- HHS may seek an injunction for breach of the DUA
- Indemnification and insurance provisions may vary if the contractor is another governmental entity

Article 6 (Cont.)

- Each party is responsible for their own legal fees and costs of enforcement
- This is the whole contract
- The contract may be automatically amended to comply with a change in the law.

Security and Privacy Inquiry (SPI)

Completed by Applicant/Bidder
Section A: Applicant/Bidder Information
Section B: Privacy Risk Analysis and Assessment
Section C: Security Risk Analysis and Assessment

Shows that applicant/bidder has basic privacy/security safeguards in place.

TEXAS Health and Human Services Commission

Any 'No' answers to questions in SECTION B and SECTION C, must be corrected by the Applicant/Bidder before Applicant/Bidder can submit a response or a complete application.
SPI goes to IT Security for review if the contract manager has any questions.

Instructions for SPI are on PCS webpage.

http://www.hhsc.state.tx.us/about_hhsc/BusOpp/HHS_SPI.pdf

PRIVACY AND SECURITY LAWS AND REGULATIONS

Federal Laws:
HIPAA (Health Insurance Portability and Accountability Act)

Covered Entity – A health plan, provider or clearinghouse. HHSC is a covered entity.

Protected Health Information – PHI is individually identifiable information and information that relates to an individual's past, present or future mental health or condition or provision of health care to the individual.

- Privacy Rule – requires an individual's authorization to use or disclose PHI except for treatment, payment or health care operations.
- Security Rule – requires technical, administrative and physical safeguards to protect PHI
- Breach Notification Rule – requires notice of breach "within a reasonable time"

HIPAA (cont.)

HIPAA requires a Business Associate Agreement when a Covered Entity contracts with a Business Associate to perform a service that requires access to the Covered Entity's (its clients') Protected Health Information

The DUA contains all of the regulatory requirements of a Business Associate Agreement. It includes citations for the applicable sections of HIPAA.

Federal Laws (cont.)

The Social Security Act establishes confidential data standards for Confidential Medicaid data. Data provided to HHSC by SSA has very stringent safeguard requirements.

SNAP and TANF regulations also protect applicant data.

IRS Publication 1075 requires that HHS ensure that Federal Tax Information is protected at all times.

Federal Laws (cont.)

42 CFR Part 2

Protects confidentiality of alcohol and substance use treatment information.

Family Educational Rights and Privacy Act (FERPA)

Protects confidentiality of educational records.

STATE LAWS

Texas Human Resources Code

- Limits use and disclosure of confidential client information to purposes directly connected with the administration of HHS's assistance programs.
- Requires rules, enforcement and safeguards to protect applicant information.

Texas Business & Commerce Code, Chapter 521 (Electronic data only)

- Requires entities that handle personally identifiable information and sensitive personal information (SPI) to safeguard it
- Requires notification of affected individuals as quickly as possible if there is a breach of system security.

Texas Administrative Code (1 TAC 202)

Department of Information Resources establishes security standards for state agencies. HHS must document and manage access to mission critical information, including client confidential information.

STATE LAWS (Cont.)

Texas Health & Safety Code Chapter 181

Includes a much broader definition of who is a Covered Entity than HIPAA.

Examples: website host, computer management entity, entities that collect, store, assemble evaluate, etc., PHI

Texas Health & Safety Code Chapter 611

Contains protections for mental health and substance use treatment records.

Texas Health & Safety Code Chapter 81.046

Protects information of persons with communicable diseases.

MONITORING
DUA COMPLIANCE

MONITORING DUA COMPLIANCE

Frequency of monitoring is based on risk.

Ideally, not less than *once a year* (or in the event HHSC suspects contractor is out of compliance), HHSC will check that the contractor is complying with contractor's duties in DUA Article 3 and the SPI.

TEXAS Health and Human Services Commission

Q & A

Questions??