TEXAS Health and Human Services

HHS Data Use Agreement and the HHS Security and Privacy Inquiry Form

Frequently Asked Questions

Updated May 19, 2021

1. What is a Data Use Agreement (DUA)?

- A DUA is a written agreement between HHS agencies and their contractors who access confidential information outlining how the contractor is to safeguard confidential information.
- In the past, HHS may have called these agreements Business Associate Agreements, but the intent is for the DUA to cover more laws than Health Insurance Portability and Accountability Act (HIPAA) and more types of non- public data.

2. Why do HIPAA-covered entities and other governmental entities need to execute a DUA?

- If a covered entity or a governmental entity is performing business associate functions for an HHS agency or accesses certain types of confidential information that have specific regulatory requirements for privacy, security, and breach notification, the HHS agency requests these entities execute a DUA so that the HHS agency contractually binds the entity to the regulatory requirements and has enforcement capability if the entity fails to protect the confidential information.

3. Who needs to execute a DUA?

- Contractors executing a contract with an HHS agency need to execute a DUA prior to contract execution.
- Medicaid providers that have already signed the Medicaid provider agreement with TMHP that do not provide any business associate functions (i.e., do not contract with any HHS agency for anything other than to provide clinical service), do not need to execute a DUA.
- Attorneys or guardians representing a Medicaid applicant or recipient do not need to execute a DUA.

4. What is considered "confidential information?"

- "Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) that consists of or includes any or all of the following:

  (1) Client Information;

  (2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information;

  (3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;

  (4) Federal Tax Information;

  (5) Personally Identifiable Information;

  (6) Social Security Administration Data;

  (7) All non-public budget, expense, payment and other financial information;

  (8) All privileged work product or other information excepted from disclosure under Chapter 552 of the Government Code;

(9) All information designated as confidential under the laws of the State of Texas and of the United States, and;

(10) To the extent permitted under the laws and constitution of the State of Texas, all information designated by HHS or any other State agency as confidential, including but not limited all information designated as confidential under the Texas Public Information Act, Texas Government Code, Chapter 552.

5. Where can I get a copy of the DUA?

- You can obtain a copy of the DUA to review on the HHS website (https://hhs.texas.gov/doing-business-hhs/contracting-hhs/vendor-resources). This form does not contain a signature block.
- The official DUA for each contract is provided to the contractor by a PCS purchaser or the HHS contract manager assigned to the specific contract and maintained in the contract file.

6. What can I negotiate or amend on the DUA?

- Nothing, unless the contractor is a governmental entity.
- In that case, you can work with your contracts attorney to alter the indemnification and insurance provisions so that they conform to state laws pertaining to governmental entities.

7. After the DUA is executed, where does it go?

- After the contract is executed, the HHS contract manager who "owns" the contract scans and uploads the contract documents, including the DUA and SPI to the HHS contract management database.

8. Who monitors contractors to make sure that they are complying with the terms of the contract, including the DUA?

- The contractor is responsible for ensuring ongoing compliance with HHS data security and privacy provisions.
- The HHS Office of the Chief Data Officer and the designated contract manager may perform periodic performance monitoring of the DUA.

9. What information is included in the DUA?

- Contract Number
- Purpose of the DUA
- Definitions
- Contractor's Obligations
- Breach Notice and Reporting
- General Provisions
- Subcontractor Agreement (Attachment 2)

10. Why do all contractors performing business associate functions need to have a DUA?

- All contractors who perform business associate functions need to have a DUA version 7.1 or higher to ensure HHS agencies are in compliance with federal law.
- A DUA helps ensure contractors are protecting agency confidential information.
- Having a DUA in place also helps to potentially reduce the number of data breaches by contractors.
- Having DUAs helps HHS agencies to respond to audits by the Department of Health and Human Services, Centers for Medicare and Medicaid Services, and the Internal Revenue Service.

11. How do I find out if existing contracts are in compliance?

- HHS agency contract staff can check the contract management database to inventory their contracts.
- If a contractor accesses HHS confidential information and there is no DUA in place or you have a DUA or BAA dated prior to March 1, 2013 (or DUA version lower than 7.1), the contractor needs to execute a DUA version 7.1 or higher.

12. How do I find out if a contractor's subcontractors are in compliance?

- Contractors are responsible for ensuring the persons/entities with whom they contract to provide services pursuant to the contractor's contract with an HHS agency are in compliance with the terms of the DUA and SPI.
- The contractor does not need to provide their subcontractor agreements to the HHS agency with whom they contract unless the HHS agency requests a copy in the event of an audit or investigation or as part of the contract monitoring process.

13. What if my contract needs a DUA?

- Agencies must notify the contractor that a DUA is required in order to continue conducting business with the agency.
- The contract manager responsible for the contractor relationship will provide the DUA to the contractor.

14. What happens if HHS does not have a DUA on file?

- If HHS is audited by federal regulatory agencies, HHS can be subject to civil monetary penalties.
- If there is a breach, the HHS agency will be held responsible for the costs of remedying the breach (credit monitoring, notification) without indemnification.
- HHS can lose federal grants and other contracts.

15. What is the HHS Security and Privacy Inquiry (SPI) form?

- The HHS SPI is required by federal and state law to demonstrate minimum compliance with privacy and security regulations. It is an attachment to the DUA.

- The form must be completed by the contractor prior to the DUA being executed.

- The short questionnaire replaces the requirement for contractors to perform a full security assessment and comply with the HHS Enterprise Information Security Standards and Guidelines (EISSG).

- The SPI form:

    - Is used for Contractors that transmit, store, and/or maintain HHS Confidential data on non-HHS systems or networks.

    - Helps HHS to identity high security risks associated with the data the contractor is accessing through this contract.

    - Helps us comply with state and federal risk assessment requirements.

    - Helps us communicate security best practices to the contractor.

    - Provides us with contact information to address security issues and needs.

    - Describes the Confidential data being handled by the contractor.

    - Is easier to understand than the EISSG, easy to fill out by the contractors security contact, and requires the contractor to review specific requirements.

16. Does the program have to remediate the risks identified in the SPI form prior to the DUA being executed?

- Risks identified by "No" responses in Sections B or C of the SPI form should be mitigated prior to executing the DUA.
- The SPI form will identify risks of the contractor handling the HHS program's confidential data. If there are any "No" responses in Sections B or C, the SPI form identifies the deadline for mitigation of those risks.
- The HHS program, in collaboration with the HHS Information Security Officer and the HHS Legal Services division, should jointly determine if any extensions may be granted to mitigate risks identified in the SPI form.
- Only the HHS program, in collaboration with the HHS Information Security Officer and the HHS Legal Services division, can determine what level of risk the program can undertake.

17. Do I need to complete the HHS SPI Form for an existing contract or for a contract renewal?

- If there is not a current Contractor-completed HHS SPI form and/or a recent security controls assessment on file with HHS, then the HHS SPI form is required. The SPI form should be updated when a change to a previous response in Sections B or C occurs.

18. Does a Contractor who uses a non-HHS computer to access Confidential Information from an HHS system need to complete the HHS SPI form?

- Yes. It is the responsibility of the HHS Information Owner and Custodian to ensure compliance with HHS security requirements when providing access to Contractors.

19. Does a Contractor who stores Confidential Information on a non-HHS laptop or workstation need to complete the HHS SPI form?

- Yes. If there is not a current Contractor-completed HHS SPI form or a recent security controls assessment on file with HHS, then the HHS SPI form is required. Please Note: Taking Screenshots of Confidential Information also qualifies as storing Confidential Information on the computer.