

**DATA USE AGREEMENT
BETWEEN THE
TEXAS DEPARTMENT OF FAMILY AND PROTECTIVE SERVICES (DFPS)
AND CONTRACTOR**

ARTICLE 1: PURPOSE AND APPLICABILITY

Data Use Agreement (“DUA”) is how DFPS obtains satisfactory assurances that the recipient (“Contractor” and/or “Authorized User”) of data from DFPS will use that information for authorized purposes as intended under this agreement. The purpose of this DUA is to facilitate access to, creation, receipt, maintenance, use, disclosure, and transmission of Confidential Information with the Contractor. This DUA describes the Contractor’s rights and obligations with respect to data use, maintenance of Confidential Information and the limited purposes for which the Contractor may create, receive, maintain, use, disclose or have access to DFPS data. This DUA describes DFPS’s remedies in the event of Contractor’s noncompliance with its obligations under this agreement. The DUA applies to all Contractors and their personnel who receive, maintain, use, disclose or have access to DFPS Confidential Information while performing services under the executed contract with DFPS. As a best practice, DFPS requires its Contractors to comply with the terms of this DUA to safeguard all types of Confidential Information.

ARTICLE 2: DEFINITIONS

For the purposes of this DUA, the underlined terms have the following meanings:

- Authorized Purpose means specific purpose(s) as described in the DUA and/or research request for the Contractor to fulfill its obligations as authorized by DFPS.
- Authorized Representative is an individual that can enter into agreement on the behalf of an organization or entity.
- Authorized User or Contractor is an individual or agency representative authorized to receive, maintain, process, view, handle, examine, interpret, or analyze Confidential Information and agrees to be bound by the provisions in this DUA.
- Breach means an impermissible use or disclosure of electronic or non-electronic sensitive personal information by an unauthorized person or for an unauthorized purpose that compromises the security or privacy of Confidential Information.
- Confidential Information means any communication or record (whether oral, written, electronically stored, or transmitted, or in any other form) provided to or made available to Contractor pursuant to the DUA. It may include, but not be limited to, information relating to a recipient of a department service or to an investigation the department conducts in performing its duties and responsibilities. In some instances, it might include information other laws or rules define as Protected Health Information or Personally Identifiable Information.
- Destroy and/or Destruction of Confidential Information, means that paper records have been destroyed and/or electronic media have been cleared, purged, or destroyed consistent with *NIST Special Publication 800-88, "Guidelines for Media Sanitization,"* such that the Confidential Information cannot be retrieved.
- Discovery means the first day on which a Breach becomes known to Contractor, or, by exercising reasonable diligence would have been known to Contractor.

- Required by Law means a mandate contained in law that compels an entity to use or disclose data or Confidential Information that is enforceable in a court of law, including court orders, warrants, subpoenas, or investigative demands.

ARTICLE 3: CONTRACTOR'S DUTIES REGARDING CONFIDENTIAL INFORMATION

1. The Contractor shall exercise the same degree of care that the Contractor uses to protect its own confidential, proprietary, and trade secret information to prevent Confidential Information from being used in a manner that is not expressly for an Authorized Purpose or as Required by Law.
2. The Contractor will access, create, maintain, receive, use, disclose, transmit, or Destroy Confidential Information in a secure fashion that protects against any reasonably anticipated threats or hazards to the security or integrity of such information or unauthorized uses.
3. The Contractor will establish, implement, and maintain appropriate procedural, administrative, physical, and technical safeguards to preserve and maintain the confidentiality and integrity of information in accordance with applicable laws/regulations relating to the prevention of unauthorized use and/or disclosure as long as the Contractor has such Confidential Information in its actual possession.
4. The Contractor must comply with all applicable federal and state laws, DFPS policies, and contract-specific requirements related to DFPS Confidential Information, including, but not limited to, the following rules and regulations:
 - a. Section 106 of the Child Abuse Prevention and Treatment Act (CAPTA), codified at 42 U.S.C. 5106a;
 - b. Section 471 of Title IV-E of the Social Security Act, codified at 42 U.S.C. 671(a)(8), and related federal rules at 45 CFR 1355.30 & 45 CFR 205.50;
 - c. Social Security Administration Data, including, without limitation, Medicaid information (The Social Security Act, 42 U.S.C. Chapter 7);
 - d. Family Educational Rights and Privacy Act, (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99;
 - e. Protected Health Information, including Electronic Protected Health Information or Unsecured Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. Chapter 7, Subchapter XI, Part C; 45 CFR Parts 160 and 164;
 - f. Confidentiality of Alcohol and Drug Abuse Patient Records, 42 U.S.C. §290dd-2; 42 CFR Part 2;
 - g. Federal Tax Information, Internal Revenue Code, Title 26 of the United States Code including IRS Publication 1075;
 - h. The Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a;
 - i. Personal Identifying Information defined by Texas Business and Commerce Code Ch. 521, and OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
 - j. Texas Family Code §261.201 and related provisions in Chapters 261 and 264;
 - k. Texas Health and Safety Code Section §81.046 and Chapters 181 and 611;
 - l. Texas Human Resources Code §12.003, §40.005, and Chapter 48;

- m. Texas Public Information Act, Texas Government Code, Chapter 552;
 - n. 40 TAC Chapter 702 Subchapter B (Child Protective Services); Chapter 707, Subchapter C, Division 4 (Child Care Investigations); and Chapter 705 Subchapter S (Adult Protective Services); and
 - o. Criminal History Record Information guidelines in the FBI's Criminal Justice Information Services (CJIS) Security Policy.
5. The Contractor agrees to disclose Confidential Information only if allowed or required by law and agrees to notify DFPS when such a disclosure is warranted. If the Contractor is asked to disclose Confidential Information to a third party, they will provide DFPS prompt notice of such request(s) no later than two (2) business days to allow DFPS to determine if protective orders and/or consent(s) to disclose requested records is warranted. The Contractor can assert its own privileges and/or objections against release of Confidential Information to a third party based on applicable law.

ARTICLE 4: SECURITY REQUIREMENTS, BREACH NOTICE AND REPORTING

Information Security Requirements.

I. General Provisions

1. The Contractor agrees to comply with all applicable state and federal laws, rules, and regulations related to the protection of data, as well as the [DFPS Data and System Security Requirements](#), which are incorporated into every DFPS contract.
2. The Contractor is responsible for safeguarding DFPS Confidential Information using administrative, technical, and physical controls that align with contractual obligations and best practices.
3. The Contractor must have internal data security procedures that include the prompt investigation of any suspected incidents and the timely reporting of findings to DFPS.

II. Best Practices and Compliance

1. The Contractor shall adhere to recognized cybersecurity best practices and frameworks to protect the confidentiality, integrity, and availability of DFPS data, including the NIST Cybersecurity Framework, NIST SP 800-53 Revision 5, the CIS Controls, and the FBI's Criminal Justice Information Services (CJIS) Security Policy.
2. The Contractor shall comply with all applicable federal and state policies, standards, and regulations concerning the confidentiality and security of data.
3. The Contractor is expected to engage in ongoing risk management and continuous process improvement, including regular security assessments and timely remediation of vulnerabilities.

III. Data Handling and Protection

1. DFPS data provided to the Contractor shall be used exclusively for fulfilling the Contractor's obligations under the executed agreement. Reuse or secondary use of data is not permitted without prior written approval from DFPS.
2. In the event of unauthorized access or loss of DFPS data, the Contractor shall notify DFPS promptly and take all reasonable steps to mitigate any harm and support DFPS in incident resolution.
3. All electronic transfer or storage of Sensitive Data must be protected using cryptographic modules validated under the current NIST 800-53 standards (e.g., FIPS 140-2 or FIPS 140-3), such as AES-256 encryption, both in transit and at rest. This includes but is not limited to data exchanged via

internal systems, external partners, or cloud services. Use of unapproved cryptographic methods or storage of unencrypted Sensitive Data is strictly prohibited. Encryption key generation, distribution, and storage must comply with applicable NIST 800-53 controls to ensure confidentiality and integrity.

IV. Training and Awareness

1. The Contractor must ensure that all personnel accessing DFPS data are properly trained on data security practices, usage restrictions, and compliance obligations.
2. The Contractor must maintain an active cybersecurity awareness program to address emerging threats and reinforce secure handling of Confidential Information.

V. Incident Response

1. The Contractor must maintain and regularly update a documented Incident Response Plan outlining procedures for handling suspected or confirmed security incidents.
2. If a security incident involves DFPS data subject to reporting under federal or state law (e.g., SSA, PII, CJIS), the Contractor must notify DFPS within 24 hours and support all required investigative and mitigation efforts.

VI. Coordination and Communication

1. The Contractor shall maintain open lines of communication with DFPS on cybersecurity matters, including potential or confirmed security incidents.
2. DFPS may schedule check-ins or meetings as needed to assess cybersecurity posture and discuss data protection practices.

VII. Data Retention and Destruction

1. The Contractor shall retain and dispose of DFPS data following applicable laws, the contract, and the DFPS Data and System Security Requirements. All destruction must comply with NIST SP 800-88 standards for media sanitization.
2. Upon contract termination or expiration, the Contractor must return or securely destroy all DFPS data unless otherwise instructed in writing.

VIII. Continuous Improvement

The Contractor is expected to regularly assess its security controls and update them in response to new threats or changes in industry best practices.

IX. Audit Clause

DFPS reserves the right to audit the Contractor periodically to ensure adherence to the DFPS Data and System Security Requirements and to confirm the Contractor's cybersecurity program aligns with industry best practices (including but not limited to NIST Cybersecurity Framework, NIST SP 800-53 Revision 5, and CJIS Security Policy). DFPS may request audit documentation or conduct onsite or remote reviews at its discretion.

X. Commitment to Cooperation

The Contractor shall cooperate fully with DFPS in all matters related to data security and breach response, recognizing the shared responsibility in protecting sensitive information.

XI. Breach Notice

1. Acquisition, access, use, disclosure, or loss of Confidential Information other than as permitted by this DUA shall be presumed to be a Breach unless the Contractor can demonstrate through a documented risk assessment that there is a low probability the Confidential Information was compromised.
2. The Contractor must maintain current privacy, security, and breach notification procedures, including an active incident response plan.
3. The Contractor must notify DFPS immediately, and no later than 24 hours, after confirmation of unauthorized access, disclosure, or use of DFPS Confidential Information.
4. The Contractor shall fully cooperate with DFPS to investigate, mitigate, and support any necessary notifications related to the Breach.
5. Upon request, the Contractor shall provide DFPS with copies of its data protection policies, procedures, and any related documentation within three (3) business days.
6. For breaches involving federal system data (e.g., Social Security Administration, Federal Tax Information), the Contractor must notify DFPS within one (1) hour of Discovery and confirm whether the breached data includes such information.
7. All breaches must be reported via email to DFPS's Security Office. The Contractor may report an incident online, by email, or by telephone.
 - Online: [Complete the Security Incident Web Based Form](#)
 - Email: infosec@dfps.texas.gov
 - DFPS Customer Service Center: 1-877-642-4777

Cybersecurity incident notifications will be treated as confidential under Texas Government Code Section 552.139, which pertains to the Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers.

ARTICLE 5: GENERAL PROVISIONS

I. Entirety of the Agreement

1. This DUA constitutes concurrence between parties for the purpose of data exchange of limited data sets. Limited data set is defined as information that excludes sensitive identifiers and might include other global identifiers.
2. This DUA is valid when executed by Authorized Representative against whom such change, waiver, or discharge is sought to be enforced. No change, waiver, or discharge of obligations arising under those documents will be valid unless in writing.

II. Subcontractor and/or Designee Agency

If this request is on the behalf of a subcontractor and/or designee agency for performance of duties on behalf of the Contractor, the subcontractor is also subject to the provisions of this DUA. Subcontractor acknowledges, understands, and agrees to be bound by the same terms and conditions applicable to the Contractor under this DUA with respect to DFPS Confidential Information. The Contractor and subcontractor (both Agency and Authorized Representatives) agree that DFPS is a third-party to applicable provisions of the subcontract. DFPS has the right, but not the obligation, to review or approve the terms and conditions of any subcontract between the Contractor and any other parties. Contractor assures DFPS that any Breach as defined by the DUA for which a Discovery occurs by the Contractor shall be reported to DFPS by the Contractor in a timely manner as outlined in the DUA.

III. Automatic Amendment and Interpretation

Upon the effective date of any amendment or issuance of additional regulations to any law applicable to Confidential Information, this DUA will automatically be amended so that the obligations imposed on DFPS and/or the Contractor remain in compliance with such requirements. Any ambiguity in this DUA will be resolved in favor of a meaning that permits DFPS and the Contractor to comply with applicable laws.

IV. Notices and Requests for Approval

All notices and requests for approval related to this DUA must be directed to the DFPS Office of Data and Systems Improvement (ODSI) at infosec@dfps.texas.gov. Contractors must complete and execute the DUA prior to any provision of *Data or Information* from DFPS and its authorized representatives.

V. Notices of Publication based on DFPS Data and Information Provided to Contractors Pursuant to a Data or Research Request

1. The Contractor, including their Authorized Representatives and designees, will inform DFPS of any publications and/or presentations that are the products and/or sub-products of data provided by DFPS. The Contractor must acknowledge that DFPS data was utilized, within reports and/or publications and must include the following statement within the reports and/or publications, including publication on a website: "The conclusions or interpretations expressed herein do not represent the conclusions, interpretations, or policies of DFPS."
2. The Contractor will not share Confidential Information or protected health information in public forums or publications. The Contractors will comply with the provisions under this DUA for both privacy, security, and confidentiality of information and data provided by DFPS.
3. The Contractor must share draft research results and conclusions with DFPS at least sixty (60) days prior to publication or distribution of any reports to allow DFPS an opportunity to review and comment and to ensure that no DFPS Confidential Information is included.

Prior to DFPS providing and/or exchanging data and/or information with/to a Contractor pursuant to a data or research request, the Contractor must provide DFPS with a list of indicators and/or data elements as part of the request. They also must outline the purpose of the data request and/or exchange, and include a brief description of either their study, project, or outline the purpose for the data request, and include/attach documents that specify the requested information.

Pursuant to this DUA, DFPS agrees to provide and/or exchange the following data and/or information with the Contractor: *[list the specific data and/or information DFPS has agreed to provide]*.

This DUA is effective as of the date that this agreement is signed by both the Contractor and DFPS.

ARTICLE 6: TERMS OF AGREEMENT

This DUA is effective as of the date the DFPS contract with the Contractor is executed and will remain in effect for the duration of that contract, unless terminated earlier by DFPS or by mutual agreement of both parties. If the underlying agreement between DFPS and the Contractor is amended or extended, this DUA will be extended concurrently to reflect the updated terms of the agreement.

If this DUA is executed as a standalone agreement in response to a data or research request and is not tied to an underlying contract, it becomes effective on the date both parties sign it and will terminate one year from the date of its execution. If the Contractor wishes to retain DFPS data beyond that period, a written justification must be submitted to DFPS for consideration. The purpose of a standalone DUA under a data

HHS0016857

Exhibit P

or research request is to allow the Contractor access to DFPS data and/or a Limited Data Set for evaluation, research, or other authorized purposes, following applicable privacy and security regulations.

Termination or expiration of this DUA will not relieve Contractor of its obligation to return or Destroy the Confidential Information as set forth in this DUA and to continue to safeguard the Confidential Information until such time as determined by DFPS. DFPS may terminate this DUA at any time by providing written notice within thirty (30) days to the Contractor. If the Contractor desires to terminate the DUA, they need to provide in writing to DFPS a plan to either return or Destroy any DFPS data.

The Contractor, as outlined in this Agreement or required by law, agrees to:

- Implement safeguards to prevent disclosure and use of Confidential Information by unauthorized parties;
- Report to DFPS any potential breaches and/or violations; and
- Require that any of its Subcontractors or agents that receive or have access to DFPS data agree to the same restrictions and conditions on the use and/or disclosure of DFPS data that apply to the Contractor under this DUA.

If there are changes in laws and regulations during the effective period of this DUA, parties agree to negotiate and/or amend in good faith material use or obligations under this DUA. Any ambiguity in this DUA will be resolved in favor of a meaning that permits DFPS and Contractor to comply with applicable laws.

The Contractor agrees to the terms under this DUA and ensures the confidentiality and security of any DFPS information provided for the purposes and/or activities including, but not limited to, performance monitoring, program evaluation, research, independent analyses, or policy reviews among others.

IN WITNESS WHEREOF, each of the undersigned has caused this Data Use Agreement to be duly executed in its name and on its behalf.

CONTRACTOR

DFPS

SIGNATURE: _____
NAME: _____
TITLE: _____
AGENCY: _____
DATE: _____

SIGNATURE: _____
NAME: _____
TITLE: _____
AGENCY: _____
DATE: _____