Privacy, Security, and Breach Notification

1.0 Definitions

"Breach" means the acquisition, access, use, or disclosure of Confidential Information in an unauthorized manner which compromises the security or privacy of the Confidential Information.

"HHSC 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 the CONTRACTOR electronically or through any other means that consists of or includes any or all of the following:

(a) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information (as these terms are defined in 45 C.F.R. §160.103);

(b) Sensitive Personal Information defined by Texas Business and Commerce Code Chapter 521;

(c) Federal Tax Information (as defined in Internal Revenue Service Publication 1075);

(d) Personal Identifying Information (as defined in Texas Business and Commerce Code Chapter 521);

(e) Social Security Administration Data (defined as information received from a Social Security Administration federal agency system of records), including, without limitation, Medicare or Medicaid information (defined as information relating to an applicant or recipient of Medicare or Medicaid benefits);

(f) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

1.1 HHSC Confidential Information

Any HHSC Confidential Information received by the CONTRACTOR under this Contract may be disclosed only in accordance with applicable law. By signing this Contract, the CONTRACTOR certifies that the CONTRACTOR is, and intends to remain for the term of this Contract, in compliance with all applicable state and federal laws and regulations with respect to privacy, security, and breach notification, including without limitation the following:

(a) Title 5 United States Code (USC) Part I, Chapter 5, Subchapter II, Section552a, Records Maintained on Individuals, The Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988;

(b). Title 26 USC, Internal Revenue Code,

(c). Title 42 USC Chapter 7, Subchapter XI, Part C, Administrative Simplification, the relevant portions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(d) Title 42 USC Chapter 7, the relevant portions of the Social Security Act;

(e) Title 42 USC Chapter I, Subchapter A, Part 2, Confidentiality of Substance Use Disorder Patient Records

(f) Title 45 Code of Federal Regulations(CFR) Chapter A, Subchapter C, Part 160, General Administrative Requirements

(g) Title 45 CFR Chapter A Subchapter C, Part 164, Security and Privacy;

(h) Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, Safeguards for Protecting Federal Tax Returns and Return Information;

(i) Office of Management and Budget Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information;

(j) Texas Business and Commerce Code Title 11, Subtitle B, Chapter 521 Unauthorized Use of Identifying Information;

(k) Texas Government Code, Title, 5, Subtitle A, Chapter 552, Public Information, as applicable,

(l) Texas Health and Safety Code, Title 2, Subtitle D, Chapter 81, Section 81.006, Funds

(m) Texas Health and Safety Code Title 2, Subtitle I, Chapter 181, Medical Records Privacy;

(n) Texas Health and Safety Code Title 7, Subtitle E, Chapter 611, Mental Health Records;

(o) Texas Human Resources Code, Title 2, Subtitle A, Chapter 12, Section 12.003, Disclosure of Information Prohibited;

(p) Texas Occupations Code, Title 3, Health Professions, as applicable;

(q) Constitutional and common law privacy; and

(r) Any other applicable law controlling the release of information created or obtained in the course of providing the services described in this Contract.

The CONTRACTOR further certifies that the CONTRACTOR will comply with all amendments, regulations, and guidance relating to those laws, to the extent applicable.

1.2 Cybersecurity Training

All of CONTRACTOR's authorized users, workforce and subcontractors with access to a state computer system or database will complete a cybersecurity training program certified under Texas Government Code, Title 10, Subtitle B, Chapter 2054, Section 2054.5192, Cybersecurity Training Required: Certain State Contractors, by the Texas Department of Information Resources.

1.3 Business Associate Agreement

CONTRACTOR will ensure that any subcontractor of CONTRACTOR who has access to HHSC Confidential Information will sign a HIPAA-compliant Business Associate Agreement with CONTRACTOR, and CONTRACTOR will submit a copy of that Business Associate Agreement to HHSC upon request.

1.4 CONTRACTOR's Incident Notice, Reporting and Mitigation

The CONTRACTOR's obligation begins at discovery of any unauthorized disclosure of Confidential Information or any privacy or security incident that may compromise Confidential Information. "Incident" is defined as an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. The CONTRACTOR's obligation continues until all effects of the Incident are resolved to HHSC's satisfaction, hereafter referred to as the "Incident Response Period".

1.5 Notification to HHSC.

(a) The CONTRACTOR must notify HHSC within the timeframes set forth in Section (c) below.

(b) The CONTRACTOR must require that its Subcontractors and contractors take the necessary steps to assure that the CONTRACTOR can comply with all of the following Incident notice requirements.

(c) Incident Notice:

1. Initial Notice.

Within twenty-four (24) hours of discovery, or in a timeframe otherwise approved by HHSC in writing, the CONTRACTOR must preliminarily report on the occurrence of an Incident to the HHSC Privacy and Security Officers via email at: privacy@HHSC.state.tx.us.

This initial notice must, at a minimum, contain:
(i) all information reasonably available to CONTRACTOR about the Incident,
(ii) confirmation that the CONTRACTOR has met any applicable federal Breach notification requirements, and

(iii) a single point of contact for the CONTRACTOR for HHSC communications both during and outside of business hours during the Incident Response Period.

2. Formal Notice.

No later than three (3) Business Days after discovery of an Incident, or when the CONTRACTOR should have reasonably discovered the Incident, the CONTRACTOR must provide written formal notification to HHSC using the Potential Privacy/Security Incident Form which is available on the HHSC website at https://hhsconnection.hhs.texas.gov/rights-responsibilities/office-chief-counsel/privacy. The formal notification must include all available information about the Incident, and the CONTRACTOR's investigation of the Incident.

1.6 CONTRACTOR Investigation, Response, and Mitigation.

The CONTRACTOR must fully investigate and mitigate, to the extent practicable and as soon as possible or as indicated below, any Incident. At a minimum, the CONTRACTOR will:

(a) Immediately commence a full and complete investigation;
(b) Cooperate fully with HHSC in its response to the Incident;
(c) Complete or participate in an initial risk assessment;
(d) Provide a final risk assessment;
(e) Submit proposed corrective actions to HHSC for review and approval;
(f) Commit necessary and appropriate staff and resources to expeditiously respond;
(g) Report to HHSC as required by HHSC and all applicable federal and state laws for Incident response purposes and for purposes of HHSC's compliance with report and notification requirements, to the satisfaction of HHSC;
(h) Fully cooperate with HHSC to respond to inquiries and/or proceedings by federal and state authorities about the Incident;
(i) Fully cooperate with HHSC's efforts to seek appropriate injunctive relief or to otherwise prevent or curtail such Incidents;
(j) Recover, or assure destruction of, any Confidential Information impermissibly disclosed during or as a result of the Incident; and
(k) Provide HHSC with a final report on the Incident explaining the Incident's resolution.

1.7 Breach Notification to Individuals and Reporting to Authorities.

(a) In addition to the notices required in this section, the CONTRACTOR must comply with all applicable legal and regulatory requirements in the time, manner, and content of any notification to individuals, regulators, or third-parties, or any notice required by other state or federal authorities, including without limitation, notifications required in Title 45 CFR Chapter A, Subchapter C Part 164, Subpart D Notification in the Case of Breach of Unsecured Protected Health Information and Texas Business and Commerce Code, Title 11, Subtitle B, Chapter 521, Section 521.053(b), Notification Required Following Breach of Security of Computerized Data, or as specified by HHSC following an Incident.

(b) The CONTRACTOR must assure that the time, manner, and content of any Breach notification required by this section meets all federal and state regulatory requirements.

(c) Breach notice letters must be in the CONTRACTOR's name and on the CONTRACTOR's letterhead and must contain contact information to obtain additional information, including the name and title of the CONTRACTOR's representative, an email address, and a toll-free telephone number.

(d) The CONTRACTOR must provide HHSC with copies of all distributed communications related to the Breach notification at the same time the CONTRACTOR distributes the communications.

(e) The CONTRACTOR must demonstrate to the satisfaction of HHSC that any Breach notification required by applicable law was timely made. If there are delays outside of the CONTRACTOR's control, the CONTRACTOR must provide written documentation to HHSC of the reasons for the delay.