Purpose

To ensure compliance with Texas Health and Human Services Commission (HHSC) privacy and security requirements for receipt, maintenance, use, disclosure, or access to confidential information.

Definitions

I. "Authorized Purpose" means the specific purpose or purposes described in the Scope of Work of the Base Contract for the Hospice to fulfill its obligations under the Base Contract, or any other purpose expressly authorized by HHS in writing in advance.

II. "Authorized User" means a Person:

A. Who is authorized to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze Confidential Information pursuant to this Data User Agreement (DUA);

B. For whom the Hospice warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to the Confidential Information; and

C. Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information as required by this DUA.

III. "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 Hospice or that the Hospice may create, receive, maintain, use, disclose or have access to on behalf of HHS that consists of or includes any or all of the following:

A. Patient Information;

B. Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information;

C. Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;

D. Federal Tax Information;

E. Personally Identifiable Information;

F. Social Security Administration Data, including, without limitation, Medicaid information;

G. All privileged work product;

H. 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.

Policy

I. If the Hospice contracts with an HHS agency and is required to sign an HHS DUA, the Hospice will meet the requirements for privacy and security as outlined in the DUA and with this policy.

II. The Hospice will cooperate with HHS agencies or federal regulatory inspections, audits or investigations related to compliance with the DUA or applicable law.

Procedure

I. The Hospice will not, without prior written approval of HHS, disclose or provide access to any Confidential Information on the basis that such act is Required by Law without notifying HHS so that HHS may have the opportunity to object to the disclosure or access and seek appropriate relief. If HHS objects to such disclosure or access, The Hospice will refrain from disclosing or providing access to the Confidential Information until HHS has exhausted all alternatives for relief.

II. The Hospice prohibits disclosure of the Hospice's work product done on behalf of HHS pursuant to the DUA, or to publish HHS Confidential Information without express prior approval of the HHS agency.

III. The Hospice will not attempt to re-identify or further identify Confidential Information or de-identified information or attempt to contact any individuals whose records are contained in the Confidential Information, except for an Authorized Purpose, without express written authorization from HHS or as expressly permitted by the Base Contract.

IV. The Hospice prohibits offshoring, or the use, disclosure, creation, maintenance or transmission of HHS Confidential Information outside of the United States of America, without express written permission from the HHS agency.

V. The Hospice will not permit, or enter into any agreement with a Business Associate to, create, receive, maintain, use, disclose, have access to or transmit Confidential Information, on behalf of the Hospice without requiring that Business Associate first execute the (HHS) Form Subcontractor Agreement which ensures that the Business Associate will comply with the identical terms, conditions, safeguards and restrictions as contained in the DUA for PHI and any other relevant Confidential Information.

VI. If the Hospice receives a request for access, amendment or accounting of PHI by any Individual subject to the DUA, it will promptly forward the request to HHS; however, if it would violate HIPAA to forward the request, the Hospice will promptly notify HHS of the request and of the Hospice's response. Unless the Hospice is prohibited by law from forwarding a request, HHS will respond to all such requests, unless HHS has given prior written consent for the Hospice to respond to and account for all such requests.

VII. The Hospice and its Business Associates will maintain an updated, complete, accurate and numbered list of Authorized Users, their signatures, titles and the date they agreed to be bound by the terms of the DUA, at all times and supply it to HHS, as directed, upon request.

VIII. The Hospice will only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form. A secure transmission of electronic Confidential Information in motion includes Secure File Transfer Protocol (SFTP) or Encryption at an appropriate level or otherwise protected as required by rule, regulation or law. HHS Confidential Information at rest requires Encryption unless there is adequate administrative, technical, and physical security, or as otherwise protected as required by rule, regulation or law. All electronic data transfer and communications of Confidential Information will be through secure systems. Proof of system, media or device security and/or Encryption must be produced to HHS no later than 48 hours after HHS's written request in response to a compliance investigation, audit or the Discovery of an Event or Breach. Otherwise, requested production of such proof will be made as agreed upon by the parties. De-identification of HHS Confidential Information is a means of security. With respect to de-identification of PHI, "secure" means de-identified according to HIPAA Privacy standards and regulatory guidance.

IX. The Hospice prohibits the storage or creation of HHS Confidential Information on free Cloud Services or social media sites, unless there is an HHS-approved subcontractor agreement including an encryption-at-rest requirement with the service or site.

X. The Hospice will provide electronic security measures to include locking a password after three failed attempts to enter the system and requiring password re-entry after 15 minutes of inactivity in all computing devices that access or store HHS Confidential Information.

XI. The Hospice will apply appropriate methods in the disposal or destruction of confidential information to ensure that information is unreadable or undecipherable (shredding, contract with a disposal company, etc.).

XII. Breach or Event Notification to HHS

A. The Hospice will cooperate fully with HHS in investigating, mitigating to the extent practicable and issuing notifications directed by HHS, for any Event or Breach of Confidential Information to the extent and in the manner determined by HHS.

B. The Hospice's obligation begins at the Discovery of an Event or Breach and continues as long as related activity continues, until all effects of the event are mitigated to HHS's satisfaction (the "incident response period").

C. Breach Notice:

1. Initial Notice.

a. For federal information, including without limitation, Federal Tax Information, Social Security Administration Data, and Medicaid Patient Information, within the first,

consecutive clock hour of Discovery, and for all other types of Confidential Information not more than 24 hours after discovery, or in a timeframe otherwise approved by HHS in writing, the Hospice will initially report to HHS's Privacy and Security Officers via email at: privacy@HHSC.state.tx.us

b. The Hospice will report all information reasonably available to the Hospice about the Event or Breach of the privacy or security of Confidential Information.

c. The Hospice will name, and provide contact information to HHS for, the Hospice's single point of contact who will communicate with HHS both on and off business hours during the incident response period.

2. Forty-eight Hour Formal Notice. No later than 48 consecutive clock hours after Discovery, or a time within which Discovery reasonably should have been made by the Hospice of an Event or Breach of Confidential Information, the Hospice will provide formal notification to the State, including all reasonably available information about the Event or Breach, and the Hospice's investigation, including without limitation and to the extent available:

a. The date the Event or Breach occurred;

b. The date of the Hospice's and, if applicable, Business Associate's Discovery;

c. A brief description of the Event or Breach; including how it occurred and who is responsible (or hypotheses, if not yet determined);

d. A brief description of the Hospice's investigation and the status of the investigation;

e. A description of the types and amount of Confidential Information involved;

f. Identification of and number of all Individuals reasonably believed to be affected, including first and last name of the individual and if applicable, the Legally Authorized Representative, last known address, age, telephone number, and email address if it is a preferred contact method, to the extent known or can be reasonably determined by the Hospice at that time;

g. The Hospice's initial risk assessment of the Event or Breach demonstrating whether individual or other notices are required by applicable law or the DUA for HHS approval, including an analysis of whether there is a low probability of compromise of the Confidential Information or whether any legal exceptions to notification apply;

h. The Hospice's recommendation for HHS's approval as to the steps individuals and/or the Hospice on behalf of individuals, should take to protect the individuals from potential harm, including without limitation the Hospice's provision of notifications, credit protection, claims monitoring, and any specific protections for a Legally Authorized Representative to take on behalf of an individual with special capacity or circumstances;

i. The steps the Hospice has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);

j. The steps the Hospice has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Event or Breach;

k. Identify, describe or estimate of the Persons, Workforce, Subcontractor, or Individuals and any law enforcement that may be involved in the Event or Breach;

l. A reasonable schedule for The Hospice to provide regular updates to the foregoing in the future for response to the Event or Breach, but no less than every three (3) business days or as otherwise directed by HHS, including information about risk estimations, reporting, notification, if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and

m. Any reasonably available, pertinent information, documents or reports related to an Event or Breach that HHS requests following Discovery.

XIII. Investigation, Response and Mitigation

A. HHS may direct the Hospice to provide Breach notification to Individuals, regulators or third-parties, as specified by HHS following a Breach.

B. The Hospice must obtain HHS's prior written approval of the time, manner and content of any notification to Individuals, regulators or third-parties, or any notice required by other state or federal authorities. Notice letters will be in the Hospice 's name and on the Hospice 's letterhead, unless otherwise directed by HHS, and will contain contact information, including the name and title of the Hospice's representative, an email address and a toll-free telephone number, for the Individual to obtain additional information.

C. The Hospice will provide HHS with copies of distributed and approved communications.

D. The Hospice will have the burden of demonstrating to the satisfaction of HHS that any notification required by HHS was timely made. If there are delays outside of the Hospice's control, the Hospice will provide written documentation of the reasons for the delay.

E. If HHS delegates notice requirements to the Hospice, HHS shall, in the time and manner reasonably requested by the Hospice, cooperate and assist with the Hospice's information requests in order to make such notifications and reports.

XIV. The Hospice will conduct privacy and security training of the workforce within thirty (30) days of hire and annually thereafter for all staff who will handle HHS Confidential Information.

A. Training will include:

1. Privacy and security policies, procedures, plans and applicable requirements for handling HHS Confidential Information,
2. A requirement to complete training before access is given to HHS Confidential Information, and
3. Written proof of training and a procedure for monitoring timely completion of training.

B. The Hospice will monitor for and correct any training delinquencies.

C. The Hospice will permit only Authorized Users with up-to-date privacy and security training, and with a reasonable and demonstrable need to use, disclose, create, receive, maintain, access or transmit the HHS Confidential Information, to carry out an obligation under the DUA for an Authorized Purpose, unless otherwise approved in writing by an HHS agency.

XV. The Hospice will sanction and maintain proof of appropriate sanctions against any staff members or Business Associates who fail to comply with an Authorized Purpose or who is not an Authorized User and used or disclosed HHS Confidential Information in violation of the DUA, the Base Contract or applicable law.

XVI. Privacy and security policies, procedures and plans will be updated following major changes with use or disclosure of HHS Confidential Information within 60 days of identification of a need for update.

Reference

Data Use Agreement- Between the Texas Health and Human Services System and Contractor (October 23, 2019)
https://hhs.texas.gov/sites/default/files/documents/doing-business-with-hhs/providers/long-term-care/nf/data-use-agreement.pdf