Performance Work Statement: COURT APPOINTED GUARDIANSHIP PETITION

OBJECTIVE: The purpose of this contract is to obtain a qualified contractor to provide Guardianship petition service for the Department of Veteran Affairs veterans. When the Department of Veterans Affairs (VA) agrees to refer a Veteran to the Guardianship Agency, the agency agrees to accept the referral. Upon acceptance by the Contractor of the referral for Guardianship petition, all terms and clauses of this Guardianship Contract shall apply until a Guardian is appointed by the Courts.

PERIOD OF PERFORMANCE: The contract will be for a potential period of performance for five (5) years, a base year and four (4) option years, based on funding availability. However, the option years may be exercised after determination that it is in the best interest of the Government, and has been determined that it is the most advantageous method of fulfilling the Government's need for these services. The contract base year and 4 optional years is estimated to begin as follows:

Base year - July 31, 2017 thru July 30, 2018
Option year 1 – July 31, 2018 thru July 30, 2019
Option year 2 – July 31, 2019 thru July 30, 2020
Option year 3 – July 31, 2020 thru July 30, 2021
Option year 4 – July 31, 2021 thru July 30, 2022

BACKGROUND/INTRODUCTION: Requirement to pursue Court appointed Guardian petition for Veterans in the hospital who lack decisional capacity and do not have family or friends willing or able to assist. Referring Social Worker Contact will include the following:

Social Worker Name: _____
Location:_____
Telephone number:_____
E-mail address:_____
Facsimile number:_____

REFERRAL POLICY: The Court Appointed Guardianship referral by Social Work Services is a key component of the Veterans Health Administration (VHA) continuum of care. The Contractor agrees to provide services in accordance with the terms and conditions stated herein, to the James A. Haley Veterans Hospital (JAHVAH), FL. Organizations who contract with the VA to provide Guardianship petition service to Veterans shall collaborate with VA staff in referral of appropriate Veterans who are deemed by the JAHVAH psychiatrist to lack decisional capacity and have no family or friends willing or able to assist. VA will maintain the right to review the Guardianship Petition process and all appurtenances by authorized VA representative(s) to ensure that acceptable standards are maintained and that the Veterans' well-being is rendered.

GENERAL REFERRAL REQUIREMENTS:

1. The Guardianship Agency shall ensure that the appointed Guardian provides the oversite for the continued health and well-being of VA Veteran. VA developed quality of care standards utilizing the standards at the following website:
http://www.va.gov/vhapublications/publications.cfm?pub=2.

2. The Guardianship Agency will have the capacity to ensure their ability to accept three (3) referrals per contract year.

3. The Guardianship Agency must be able to accept VA referrals in a timely fashion (ideally within 24 hours of request). The per case rate(s) established within the terms of this contract will include the cost of the petition and all guardianship proceedings on behalf of the Veteran. Every effort shall be made to ensure the Veteran under Guardianship is in a setting that achieves an optimal level of care and well-being.

TERMINATION OF SERVICES: VA reserves the right to remove any or all VA patients from the Guardianship Agency at any time when it is determined to be in the best interest of the VA or the Veteran without additional costs to the Government.

VA AUTHORIZATIONS: Authorization for Court Appointed Guardianship Petition will be submitted by Social Work Service. Each referral and authorization validity will be noted on the invoice with a total cost of the petition and submitted through OB 10 at: https://www.vis.fsc.va.gov

HIPAA COMPLIANCE: HIPAA compliance is required. The Contractor must adhere to the provisions of Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the National Standards to Protect the Privacy and Security of Protected Health Information (PHI), as required by HIPAA. The Department of Health and Human Services (HHS) has promulgated rules governing the security and use and disclosure of protected health information by covered entities, including the Department of Veterans Affairs (VA). In accordance with HIPAA, the Contractor may be required to enter into a Business Associate Agreement (BAA) with VA Facilities as an entity that does not require a BAA as long as they are conducting health care on VA's behalf. The Department of VA shall enforce that Contractor must remain in 100% compliance with all of HIPAA requirements.

AGENCY REQUIREMENTS - STATE LICENSURE: The Agency will obtain an attorney to petition the Courts and file paperwork for appointment of a guardian. The Agency will follow through with the petition and appear in Court as the recommended guardian and be appointed as the Guardian. All travel to and from the Courts is the responsibility of the Agency. The Agency will maintain guardianship of the Veteran until the Veteran either expires or is declared competent. The Agency must maintain a current and unrestricted state license as needed for all personnel serving in a legal capacity for the Agency. Changes in the status of the licensure must be immediately reported to the JAHVAH Social Work Department POC and the Contracting Officer.

VA ACTIONS REGARDING SERIOUS QUALITY OF CARE DEFICIENCES: In cases of serious deficiencies affecting the health or safety of Veterans or in cases of continued uncorrected deficiencies, VA will take one or more of the following actions in accordance with the terms and clauses of the Guardianship and applicable procurement regulations:

a. Increase VA staffing monitoring until the State agency clears the deficiency

b. Suspend future Veteran referral for Guardianship petition to the Agency

CHARITABLE CONTRIBTIONS: The Guardianship Agency will not solicit contributions, donations, or gifts from Veterans or family members. Note: Established charitable fundraising activities of the Guardianship Agency fall outside the scope of this language.

VA PAYMENTS: VA agrees to make payment on a timely basis for services rendered in accordance with such authorizations upon receipt of proper invoices submitted by the Guardianship Agency as outlined in this contract. Payments made by VA constitute the total cost of Guardianship Petition. No additional charges will be billed to the Veteran or his/her beneficiary, family, either by the Guardianship Agency or any third party without specific prior authorization in writing from the VA facility authorizing the transaction.

Invoices will be sent by email, fax, or mailed to:

Department of Veterans Affairs
Attn: Social Work Service (122), Guardianship
13000 Bruce B. Downs Blvd.
Tampa, FL 33612

QUALITY ASSURANCE SURVEILLANCE PLAN: The Quality Assurance Surveillance Plan (QASP) was developed to evaluate Contractor actions while implementing the Performance Work Statement (PWS). The QASP is designed to provide an effective surveillance method of monitoring Contractor performance for each listed objective on the Service Delivery Summary (SDS) included in this contract. The QASP provides a systematic method to evaluate the services the Contractor is required and has agreed to furnish. The Government desires to maintain a quality standard in providing primary care/mental health services to its patients. The resulting contract is considered the best means of achieving that objective. Contractor agrees to take full responsibility and adhere to the following:

a. The Contractor, and not the Government, is responsible for management and quality control actions to meet the terms of the contract.
b. The role of the Government is quality assurance to ensure contract standards are achieved.
c. Contractor will be subject to performance standards specified in the Quality Assurance Surveillance Plan (QASP).

VA INFORMATION CUSTODIAL LANGUAGE:

1. Information made available to the contractor or subcontractor by for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and is prohibited for use in any other context without prior written agreement by an approving official representative of the VA.

2. This clause expressly limits the contractor/subcontractor rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

3. Under no circumstances should any VA information be co-mingled with any other data on the contractors/subcontractor's information systems or media storage systems to ensure VA requirements related to data protection and media sanitization are met.

4. VA reserves the right to conduct on-site inspections of contractor and subcontractor Informational Technology (IT) resources to ensure data security controls, separation of data and

job duties, and destruction/media sanitization procedures are in full compliance with VA directive requirements.

5. Prior to termination or completion of this contract, Contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA.

6. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable, VA Records Control Schedules, VA Handbook 6500.1 and Electronic Media Sanitization.

7. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

8. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies.

9. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

10. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

11. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

12. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.1, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

13. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

14. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

15. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

16. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above-mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

17. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

SECURITY INCIDENT INVESTIGATION:

1. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

2. To the extent known by the contractor/subcontractor, the contractor/subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

3. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

4. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

LIQUIDATED DAMAGES FOR DATA BREACH:

1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

2. The contractor/subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non- Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

3. Each risk analysis shall address all relevant information concerning the data breach, including the following:

a. Nature of the event (loss, theft, unauthorized access);
b. Description of the event, including:
c. Date of occurrence;
d. Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
e. Number of individuals affected or potentially affected;
f. Names of individuals or groups affected or potentially affected;
g. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
h. Amount of time the data has been out of VA control;
i. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
j. Known misuses of data containing sensitive personal information, if any;
k. Assessment of the potential harm to the affected individuals;
l. Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate.
m. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.
n. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the VA liquidated damages for affected individual to cover the cost of providing credit protection services to affected individuals:

SECURITY CONTROLS COMPLIANCE TESTING:

1. On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract.

2. With 10 working-days' notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General.

3. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

TRAINING:

1. If applicable, all contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete VA Privacy and Information Security Awareness and Rules of Behavior Training and Privacy and HIPAA Training and HIPAA Training before being granted access to any veteran information and if authorized, its systems.

2. All contractor employees must sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Rules of Behavior before being granted access to VA information and if authorized, its systems.

3. The contractor shall provide the contracting officer and/or the COR a copy of the training certificates and certification of signing the Rules of Behavior for each applicable employee within seven days of the initiation of the contract and annually thereafter, as required. Contract performance will be monitored, evaluated, and annotated on the VA Quality Assurance Surveillance Plan annually or more frequent as needed.

4. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

5. The Certification and Accreditation (C&A) requirements do not apply and a Security Accreditation Package is not required for this PWS.

SECURITY REQUIREMENT FOR CONTRACTOR EMPLOYEES: Identification of qualified staff/personnel to work directly with referred Veterans as outlined in the Performance Work Statement and achievement of VA Contractor staff through VA Human Resources processes. This status allows the contractor staff the ability to access required systems and information necessary to perform work required including but not limited to:

1. Security/background investigations via NACI (National Agency Check with Inquiries) and SAC (Special Agreement Check) that includes electronic fingerprinting for contracted housing personnel providing care, supervision, and/or transportation to Veterans. Contractor must provide each staff member's date of birth, social security number, hair color, eye color, address, phone number, e-mail address, and proof of U.S. citizenship or legal residency status for the security/backgrounds investigation process to initiate. Contractor is reminded to figure the cost of the employee background investigations into their price quotation. The price is subject to change during the term of the contract.

2. Should the investigation be conducted by the Office of Personnel Management (OPM), the Contractor shall reimburse the VA within 30 days.

3. Systems status for case managers and supervisors at the VA are for documentation purposes. In order to achieve system status, each staff member must complete a credentialing process at the local VA medical center (i.e. Vet Pro). Vet Pro is necessary for all licensed, registered or certified clinical staff members. After the contract is awarded, staff must be in direct contact with VA Human Resources personnel to begin the process online. A federal Personal Identification Certification card will also be issued which requires a face-to-face visit to the local VA medical center for verification of documents and photographs of the individual staff member. Contractor must immediately inform Contracting Officer Representative, Contracting Officer, or ADATP Administrative staff of any changes or new hiring of staff. Contractor shall ensure all new employees possess active licensure and/or certification to fulfill duties of position assigned.

4. The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the contract.

5. Failure to comply with the contractor personnel security requirements may result in termination of the contract for default.

PRIVACY TRAINING & OTHER REQUIRED TRAININGS: Due to increased emphasis on privacy and information security, the Privacy Policy Awareness Training was established and applied to all new and existing contracts awarded by the Department of Veterans Affairs. Contractor is responsible for providing all documentation of completed Privacy Policy Awareness Training that is completed by each Contractor employee working under this contract to the Contract Office (CO). The following documentation must be included in the contract file at all times for verification purposes if needed:

• Completion of VA's on-line Information Security and Privacy combined Awareness Training Course and the Privacy Policy Awareness Training Course for case managers and their supervisor working directly with Veterans under this contract. The Privacy Awareness Training requirement shall be fulfilled under additional privacy awareness training options. To complete the online VA Privacy and Information Security Training, Contractor staff must establish a VA Employee Education System account which can be completed online. The Privacy Awareness Training is in addition to any other training that may be required of the Contractor and subcontractor(s).