1. Scope of Work

1.1 The contractor shall provide all labor, personnel, equipment including confidential containers (consoles/bins), supplies, secured vehicles, materials, supervision, and other related services necessary to provide on-site commercial document destruction services for confidential waste (administrative papers, classified papers, sensitive documents, hard bound journals, magazines, CD's and white and mixed paper) at the Veterans Affairs Central California Health Care System(VACCHCS) and Five Outpatient Clinics.

1.2 VACCHCS personnel in all locations are in the practice of putting all confidential, sensitive or administrative documents, as well as other paper, in locked containers located throughout all of the VACCHCS facilities.

2. Place of Performance

VA Fresno 2516 E. Clinton Ave Fresno, CA 93703	VA South Valley 1050 N. Cherry Ave Tulare, CA 93274	VA Oakhurst Clinic 40597 Westlake Drive Oakhurst, CA 93644
VA North Valley Clinic 340 E. Yosemite Ave. Merced, CA 95340	Human Resources Shaw Forty One Center 155 E. Shaw #100 Fresno, CA 93710	VA Visalia Clinic 561 S. Pinkham Street Visalia, CA 93292

Period of Performance:

Base Year:	October 1, 2016 to September 30, 2017
Option Year 1:	October 1, 2017 to September 30, 2018
Option Year 2:	October 1, 2018 to September 30, 2019
Option Year 3:	October 1, 2019 to September 30, 2020
Option Year 4:	October 1, 2020 to September 30, 2021

3. Security Waste Pick up Schedule Locations and Quantities of Containers

3.1 Pick-up of security waste shall be accomplished in accordance with the pick-up schedule listed in paragraph 3.2 and 3.3

3.2 Location and Time (Monday through Friday during Normal duty hours 8:00AM-3:30PM)

VA Central California HCS	See schedule below
VA South Valley Clinic	Bi-weekly
VA Oakhurst Clinic	Bi-weekly
VA North Valley Clinic	Bi-weekly
VA Homeless Center	Weekly
VA Visalia Clinic	Monthly

VA Central California facility requests service on a regular schedule date of containers or consoles, to be emptied when the bins are ¾ (three-quarter) full.

Schedule for VA Central California locations;
Main Hospital, Bldg. 1, Trailer LC2, and All Buildings to be Serviced once a week.

High volume areas, will be Serviced twice a week;

HIM, Basement, B1A01
Emergency Area, Basement
Pharmacy Area, 1st Floor, 1B061
Laboratory Area, 2nd Floor, 2B24
Cardiology Area, 2nd Floor, 2C08
5th Floor (West & East Units)
Trailer LC2, Non-VA area, corridor #4

3.3 When regular delivery / pick up days occur on one of the Federal holidays listed below, the regular delivery / pick up shall automatically shift to the following business days (Monday through Friday). The ten national holidays observed by the Federal Government are:

New Years Day	1 January
Martin Luther King Jr Day	Third Monday in January
Presidents Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veterans Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

3.3.1 Any other day specifically declared by the President of the United States to be a national holiday. If a holiday falls on Sunday, the following Monday will be observed as the legal holiday. If a holiday falls on Saturday, the preceding Friday is observed as a legal holiday by U.S. Agencies

3.4 In the event of schedule changes and prior to any changes made to the schedule, the Contracting Officer Technical Representative (COTR) will notify the Contracting Officer (CO) in writing of the revised pick up schedule. A revised pick-up schedule will be provided to the contractor in writing along with the contract modification from the CO.

3.4.2 The contractor shall only be invoicing and receiving payment for containers/consoles/bins that are 100% emptied. In the event, the contractor fails to empty a container, the contractor will have 24 hours (weekdays) once notified to empty the container. The COTR will have the authority to change bin sizes, as needed.

3.4.3 The contractor will provide two additional 95 gallon containers to the VA Facility in order to service customers on days that the contractor is not scheduled for pick up, due to unforeseen situations.

3.5 Quantity of Containers per location

Service site	Large, 32”	Medium, 26”	Small, 16”
VA Fresno	129	22	13
VA Fresno, new / replacements	11	4	0
VA South Valley Clinic	2	0	0
VA Oakhurst	3	0	0
VA North Valley Clinic	3	0	0
VA Shaw Ave	2	0	0
VA Visalia Clinic	2	0	0

3.6 Shredding Specifications

3.6.1 The Contractor shall be National Association for Information Destruction Certified (NAID).

3.6.2 The Contractor shall provide shredding document destruction services for all secure waste that are collected in locked containers; (administrative papers, classified papers, sensitive documents and CD's).
3.6.3 Shredding of all documents must meet or exceed the following criteria based on VACCHCS requirements and the requirements set forth by NAID (National Association of Information Destruction):

- Cross-Cut or Pierce and Tear:
  Width (max): ¾ inch & Length (max): 2 ½ inches
- Continuous Shred:
  Width (max): 5/8 inch & Length (max): Indefinite
- Pulverized, Disintegrator or Hammermill:
  Screen Size (max): 2-inch diameter holes

3.6.4 Definitively destroying the records means the material cannot be reassembled and used in an inappropriate manner in violation of law and regulation. Sensitive records are records that are national security classified or exempted from disclosure by statute, including the Privacy Act, or regulation. Information protection, destruction precautions, the documents (paper data), VACCHCS information containing social security number and other information covered by the privacy act shall be destroyed.

3.7 Incident Notification

3.7.1 The contractor shall notify VACCHCS's COTR within 24 hours of Contractor's discovery of any incident, which may potentially be a data breach, including a HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of Protected Health Information (PHI), whether secured (PHI which has been destroyed or in the alternative has been rendered unreadable, unusable or undecipherable) or unsecured (PHI) not secured through the use of a technology which renders it unusable, unreadable, or indecipherable through methodology specified by HHS in guidance issued under § 13402(h)(2) of the HITECH Act), not provided for by this Agreement and promptly provide a report to VACCHCS within ten (10) business days of the notification.

3.8 Quality Control

3.8.1 The contractor shall develop and maintain quality programs to ensure recycling services are performed in accordance with commonly accepted commercial practices and comply with VACCHCS requirements. The contractor and COTR will conduct quarterly inspections, in order to meet VA Environmental of Care Inspection. 100% of the containers/ consoles/bins must be emptied and shredded at each location per the schedule provided by the COTR. If a container, console/bin is not emptied and shredded, the contractor shall notify the COTR, of the reason that a console/bin could not be emptied and shredded. The contractor shall only be invoicing and receive payment for containers/consoles/bins that are 100% emptied. The contractor shall remove bins from Facility, after service is complete before 3:30pm.

3.9 Safety

The contractor shall have in place a documented and comprehensive Health and Safety program to ensure all shredding activities are provided in a safe and secure manner. As a commitment to safety the

contractor must be working towards achieving the Occupational Safety and Health Administration's (OSHA) Voluntary Protection Program (VPP) Certification.

3.10 Contractor Vehicles

3.10.1 All contractor vehicles utilized in the performance of this contract shall maintain insurance (up to the minimum coverage required by the respective state) and shall maintain current state vehicle registration.
3.10.2 All contractor employees shall possess a valid California state driver's license and have a clean driving record. The contractor or his/her employee's while performing under this contract shall use no personal vehicles to transport containers to and from the government and contractor site.

3.10.3 The contractor shall ensure that all contractor vehicles utilized for this performance contract are kept in proper working condition. The contractor vehicles shall be locked and properly secured at all times while at the government site or in route to and from contractor site. Vehicles used in the performance of the contract shall not be left unattended and unlocked at anytime while transporting VACCHCS security waste.

3.11 Contractor Facilities

3.11.1 All security waste shall be shredded onsite at the VACCHCS premises. In the event that onsite shredding is not available due to unforeseen mechanical issues, the confidential materials are to be left on VACCHCS premises, and COTR is to be notified. The contractor must schedule an onsite vehicle within 48 hours.

3.11.2 Prior to beginning performance of the contract, the designated contractor facility be the destruction site will be inspected by COTR and the VACCHCS's Privacy Officer and approved in writing by the VACCHCS at the contractor facility, and until completion of destruction, the security waste material must be maintained in a secured holding area all times to prevent any disclosure or unauthorized access.

3.12 Security Waste Collection Containers and Phase-Out for Follow-On Contracts

3.12.1 The size of the containers provided is referenced in paragraph 3.5.

3.12.2 The lockable containers shall be kept locked at all times. The contractor shall provide two sets of keys for each lockable security waste container. One set of keys shall remain in the possession of the contractor or his employees at all times while at the Contractor's site. One set of keys shall be provided to the VACCHCS COTR.

3.12.3 In the event the Government awards a follow on contract to other than the incumbent contractor, the contractor will cooperate to the extent required to allow for an orderly changeover to the successor contractor. This transition shall be as smooth and transparent as possible to ensure no interruption in the services currently being provided.

3.12.4 In the event the Government awards a follow on contract to other than the incumbent contractor. The incumbent contractor shall schedule a time with the COTR to remove containers/consoles/bins throughout the VACCHCS facilities at no additional cost to the government.

3.12.5 The contractor shall deliver the required number of lockable security waste containers (Joint Commission compliant) with keys to the VACCHCS site specified in the contract within 5 calendar days after contract award and approval of VACCHCS security suitability. The confidential waste containers

shall be placed at the designated locations directed by the COTR or the local VACCHCS site point of contact (POC). The VACCHCS site POC will be provided to the contractor by the COTR. All containers must have a baffle preventing anyone from pulling documents out of the containers.

3.12.6 The contractor shall submit one point of contact for all locations to the COTR within 5 days of contract award.

3.13 VACCHCS Clearance Requirements

The contractor shall be required to comply with all security requirements of VACCHCS. All security requirements must be met, and the employees must be cleared prior to the contractor performing work under the contract. Employees that cannot meet the security requirements and clearance requirements will not be allowed to perform work under this contract. Upon contract award, COTR will assist awardee to ensure the appropriate type of background investigation and/or fingerprints are initiated, and ultimately completed, on contract personnel in accordance with the contract terms and conditions and the VA/VHA Directive and Handbook 0710 Series. This also includes any required training for contract personnel (e.g. VA Cyber Security Awareness, VHA Privacy Policy, etc.) including Compliance and Business Integrity (CBI) Training.

3.14 HIPAA Compliance – Covered Entities

Under HIPAA Privacy and Security Rules, the Contractor providing services under this contract is considered to be a "covered entity," and thus is not required to enter into a Business Associate Agreement with VA. However, the Contractor must observe Public Law 104-191 and all respective regulations implementing this law while providing services under this contract.

3.15 Handling of Records

3.15.1 Information or records accessed and/or created by the Contractor in the course of performing services under this contract are the property of the VA and shall not be accessed, released, transferred, or destroyed except in accordance with applicable federal law, regulations, and/or VA/VHA policy. The Contractor will not copy information contained in VA information systems, either by printing to paper or by copying to another digital format, without the explicit instruction and written approval from of the officials listed in paragraph a., above, except as is necessary to make single copies in the ordinary course of providing patient care. The Contractor will not commingle the data from VA information systems with information from other sources. Contractor shall report any unauthorized disclosure of VA information to the Contracting Officers Technical Representative (COTR).

3.15.2 The Logistics Management Service will follow VACCHCS procedures to assure VA sensitive information is protected.

3.15.3 The C & A requirements do not apply, and that a Security Accreditation Package is not required.

3.16 See attachment one for NCA- Contractor Personnel Security Requirements

3.17 See attachment two for Wage Determination

3.18 See attachment three for BAA

1. GENERAL

Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.
b. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.
c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.
d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.
e. The contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor's employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

3. VA INFORMATION CUSTODIAL LANGUAGE
a. Information made available to the contractor or subcontractor by VA 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 shall not be

used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on-site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
c. 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. 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, and VA Handbook 6500.1, *Electronic Media Sanitization*. 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.
d. 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. 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.
e. 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.
f. 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.
g. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
h. 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.

i. 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.
j. 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.
k. 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.
l. 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 COTR.

6. SECURITY INCIDENT INVESTIGATION

a. 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 COTR 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.

b. 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.

c. 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.

d. 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.

7. LIQUIDATED DAMAGES FOR DATA BREACH

a. 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. However, it is the policy of VA to forgo collection of liquidated damages in the event the contractor provides payment of actual damages in an amount determined to be adequate by the agency.
b. 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.
c. Each risk analysis shall address all relevant information concerning the data breach, including the following:
(1) Nature of the event (loss, theft, unauthorized access);
(2) Description of the event, including:
(a) date of occurrence;
(b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code; (3) Number of individuals affected or potentially affected;
(4) Names of individuals or groups affected or potentially affected;
(5) 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;
(6) Amount of time the data has been out of VA control;
(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
(8) Known misuses of data containing sensitive personal information, if any;
(9) Assessment of the potential harm to the affected individuals;
(10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
(11) 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.
d. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the VA liquidated damages in the amount of **$37.50** per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
(1) Notification;
(2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
(3) Data breach analysis;
(4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
(5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

(6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

9. TRAINING

a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

(1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix E relating to access to VA information and information systems;

(2) Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;

(3) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

(4) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

b. The contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. 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.