Statement of Work (SOW) Worksheet

1. **PR # / TITLE: 654-18-1-225-0001 St. Jude Ilumien OCT Service Contract**

2. **BACKGROUND:** Contract maintenance services are required to service the medical equipment/support systems listed in Section 3 of this document. There are no VA employees trained or qualified to perform this work.

3. **DESCRIPTION AND SCOPE OF WORK:** The contractor shall furnish a Service Contract to include support labor, technical support, travel expenses, and expertise necessary to support annual preventive maintenance and all unscheduled repairs of Ilumien OCT system located at VA Sierra Nevada Health Care System (VASNHCS) located at 975 Kirman Ave, Reno, NV 89502. Service contract will provide parts and labor to the systems identified in this SOW. Description of system and options to be covered under this service agreement:

Description	Model#	Serial #	Manufacturer
ILUMIEN O.C.T.	C7-XR	C7XR-11-06-146	ST.JUDE / ABBOTT

4. **DELIVERABLES SCHEDULE**

a. Contract period shall be for one year from award of purchase order, 1 OCT 17 through 30 September 18. Four additional option years on contract.

b. Preventive maintenance visits will be completed annually in the month mutually agreed upon by the customer and service contractor. PM to be performed within manufacturer's specifications.

c. Parts replacement coverage.

d. Provide loaner system as needed for service/repair of covered system.

e. Ability to provide remote systems diagnostics and maintenance.

f. Contractor response times for repair calls:

1) Initial telephone response will be less than 15 minutes

2) If the contractor's telephones are not answered by technical personnel, a technical maintenance representative will respond by telephone to VASNHCS within one hour of receiving a service call.

3) On-site service response time will be within 72 hours.

4) Provide 24x7 Telephone Technical Support for covered device.

Statement of Work (SOW) Worksheet

5. **CONTRACTOR RESOURCE REQUIREMENTS & QUALIFICATIONS**

   a. Service providers must have been engaged in maintaining/ servicing the equipment listed in Section 4 for a minimum of 2 years. Field service representatives must provide, upon request, evidence of appropriate training for the equipment they are servicing.

   b. Subcontracting of maintenance services will not be allowed without coordination with the contracting officer's technical representative (COTR) and written permission of the Contracting Officer.

   c. The service contractor will maintain a sufficient parts inventory to keep equipment downtime to a minimum. The inventory will be replenished as needed to support the services outlined on this statement of work.

   d. Parts replaced by the contractor become property of the contractor unless required to be maintained by VASNHCS due to on-going evaluation of equipment/system identified on incident report or sentinel event. Hard drives will be retained by the VA.

   e. Contractor will provide the necessary manpower and supervision to properly execute the maintenance and repair program.

   f. Service providers must use test equipment that is within calibration.

   g. The service contractor must have legal access to OEM proprietary diagnostic software. Only SW validated for the devices listed in paragraph 4 shall be used.

   h. Only manufacturer approved factory service parts shall be used.

6. **PERFORMANCE STANDARDS AND QUALITY ASSURANCE**

   a. Service contractor must furnish all tools and materials (e.g., service manuals, diagnostic software, etc.) required to service the equipment to manufacturer's specifications.

   b. Documentation of Service: - At the conclusion of each scheduled or unscheduled repair the contractor will provide a written service report indicating the date of service, the model, serial number and location of equipment serviced, the name of the representative, and the services performed and parts replaced. The reports will be delivered to the Biomedical Engineering Office, located at 975 Kirman Avenue, Reno, NV. The office is located in Building 1, Room C4282. Service may also be emailed to matthew.jones4@va.gov

Statement of Work (SOW) Worksheet

c. Service contractor to provide preventive maintenance (PM) service per manufacturer specifications.
   1) PM inspections will be performed by the contractor annually on all equipment and support systems listed in Section 4.

   2) Service to include system inspection, calibration as necessary, system lubrication and filter replacement or cleaning.

   3) Upon completion of PM inspections, equipment will be labeled with a signed and dated preventive maintenance/electrical safety inspection sticker.

d. Service documentation - A documentation package acceptable for JOINT Commission purposes will be maintained by the contractor and made available to VASNHCS. Required documentation includes:

   1) Service Histories. The contractor will maintain a permanent record of service histories for equipment listed in Section 4.

   2) Preventive Maintenance inspections. The service contractor will have written procedures to be followed and documented evidence that equipment/systems listed in Section 4 have been inspected according to those procedures.

   3) A preventive maintenance inspection report will be prepared and delivered to the contracting officer's technical representative (COTR) annually. This report will show all equipment by serial number as well as all parts replaced on each system.

e. Service contractor will provide all services necessary to provide timely corrective action on all manufacturer hazard alerts/recall notices.

f. Normal hours are from 7:00am - 4:30 PM, Monday – Friday, except Federal Holidays. Contractor may work outside normal business hours by arrangement with Biomedical Engineering if such services are provided without additional charge to the government, or if after-hours service is a service covered under the contractor's maintenance agreement. Contractor may also work outside of normal business hours if a request for services outside of the scope of this contract is coordinated with Biomedical Engineering.

g. VASNHCS Biomedical Engineering will work with the service contractor to provide a designated area for the purpose of servicing the equipment listed in Section 4. In most cases work will be performed in the area where the equipment is used for patient care.

h. INSURANCE/WARRANTIES: The expectation is that the service contractor will provide the industry standard 90 day warranty for repairs/services.

7. **LOCATION OF WORK AND TRAVEL**

a. Contractor Check-In: - The contractor's representative will contact Biomedical Engineering at (775)784-3940 prior to performing any maintenance services.

b. Work to be performed will be at VA Sierra Nevada Health Care System, Main campus located at 975 Kirman Avenue, Reno, NV.

8. **SECURITY REQUIREMENTS**

a. The service representative(s) will be required to sign in with the VA Police and be issued a temporary badge for each service visit.

b. Patient health information is not stored on this device.

c. This medical device is a **stand-alone** unit and does **not connect to a network.**

9. **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.

10. **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.

11. **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.

12. 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.

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.

13. **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.

15. **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.