## STATEMENT OF WORK

## Title

Novel Exoskeleton Controllers Design & Development and Advanced Rehabilitation Robot for RTT Use and Research at Rehabilitation Research & Development Services Center for Limb Loss and MoBility (CLiMB) of VA Puget Sound Health Care System.

## Background

CLiMB seeks to advance rehabilitation for Veterans Having survived Stroke through Robot-Mediated Repetitive Task Training (RTT) in acute and sub-acute stages of recovery. Stroke causes significant long-term disability. The incidence of stroke in the Veteran population is very high, with approximately six-thousand VA admissions for Acute Ischemic Stroke in 2014. Developing efficacious rehabilitation programs for Veterans is a high priority. For this contract and related project, the goal is to improve upper extremity functional performance which has the potential to impact Veterans’ Activities of Daily Living (ADL) and in turn, improve their vocation, recreation, and overall quality of life.

Previous research indicates that to significantly affect Stroke Recovery, it is pertinent to initiate RTT in the acute and sub-acute stages of Stroke Recovery to maintain healthy joint coordination while keeping patients both positively engaged and challenged. Repetitive Task Training is more effective than simple joint movements in improving upper extremity (arm) function. Non-robot mediated RTT can be tedious for the clinician and patient, as it can take many repetitions for ultimate results.

The VA seeks to advance their current healthcare services for Veteran stroke patients, by incorporating Robot-Mediated Repetitive Task Training, via the Harmony SHR which is a bilateral upper extremity exoskeleton Advanced Rehabilitation Robot. The University of Texas at Austin will provide one of these for the term of the contract, for use by VA Clinicians, Principal Investigators, and their Assistants and Students that will aid in the ease, effectiveness, and overall experience of post stroke rehabilitation therapy for their patients. The Harmony SHR, has the ability to deliver bi-manual three-dimensional (3D) arm therapy, as treatment for early stroke recovery stages. Previously, available treatment options in the field have lacked the proper RTT tools that deliver and maintain joint coordination during 3D arm movement, while ensuring the assistance commensurate with patients’ abilities. Training to use The Harmony SHR will be provided by Dr. Deshpande who will also be available in the event the need for troubleshooting should arise.

**Objective**

The Contractor shall work with VA to develop Novel Controllers that use promising neurological basis for training to facilitate RTT while ensuring correct movement patterns in acute and sub-acute stage stroke patients. Specifically, (1) a Synergy Avoidance (SA) Novel Controller that will apply joint torques to push the patients away from the maladaptive joint coordination (only interfering with the movements once the subject initiates such a maladaptive movement strategy); and (2) a Task Assistance (TA) Novel Controller that will apply assistive joint torques to directly help stroke patients achieve 3D RTT activities with correct coordination at a high intensity (repetitions per session). These two Novel Controllers will be developed by Dr. Deshpande at the laboratory in the Department of Mechanical Engineering at University of Texas at Austin. This is the primary task of the contract, to develop the SA and TA software, install the software into the Harmony SHR’s Computer, and provide the Harmony (with training), to the VA.

New rehabilitation programs that improve upper extremity functional performance have the potential to impact Veterans’ Activities of Daily Living (ADL) and improve their vocation, recreation, and overall quality of life. The development of the SA and TA Controllers constitutes a novel contribution from a robotics perspective since SA and TA Controllers have not yet been fully addressed. The SA Controller has the potential to shift the way in which robotic and non-robotic therapy is delivered, to target the underlying neural maladaptive strategies of Stroke Rehabilitation. This project may serve as a key ingredient to uncovering an understanding of neuro-recovery and for delivering previously unavailable treatments to Veterans.

## Scope

The general scope is that the Contractor, University of Texas at Austin be responsible to develop for VA Puget Sound Health Care System the novel exoskeleton controller design, deliver the Harmony and ensure functional use, build and execute protocols for stroke therapy and data analysis, and work with the VA Research Team to disseminate the research. In “Tasks” below, and in accordance with the Item Schedule of this contract, the Contractor is to perform for the base year with one optional year, these tasks.

**Tasks**

Base Year (May 15th, 2024 to May 14th, 2025)

1: The Contractor shall develop (at laboratory in the Department of Mechanical Engineering at University of Texas at Austin), install, and ensure working order of a Synergy Avoidance (SA) Novel Controller within Harmony SHR Computer System.

2: The Contractor shall develop (at laboratory in the Department of Mechanical Engineering at University of Texas at Austin), install and ensure working order of a Task Assistance (TA) Novel Controller within Harmony SHR Computer System.

3: The Contractor shall deliver (with Novel Controllers), install, and ensure working order of Harmony SHR at VA Puget Sound Health Care System. The estimated delivery is by May 30th, 2024, or 15 days after contract award.

4: Aid in Harmony SHR set up and train the VA CliMB Research Staff on use of Harmony SHR, to include as needed availability and any troubleshooting for Harmony SHR exoskeleton or its software by June 15th, or 15 days after delivery).

5: Collaborate on data analysis and dissemination with CLiMB Research Staff.

6: Dr. Deshpande (Contractor) shall mentor and supervise project-specific VA CLiMB Research Assistants.

Option Year 1 (May 15th, 2025 to May 14th, 2026)

1: Provide as needed availability and any troubleshooting for Harmony SHR exoskeleton or its software.

2: Collaborate on data analysis and dissemination with CLiMB Research Staff.

3: Dr. Deshpande (Contractor) shall mentor and supervise project-specific VA CLiMB Research Assistants.

## Security Requirements.

The contractor employees shall not have access to VA sensitive or computer information and will not require routine access to VA Facilities. The contractor employees shall require intermittent access only and will be escorted by VA employees while at VA Facilities. No background investigation is required.

## Government-Furnished Equipment (GFE)/Government-Furnished Information (GFI).

There will be no GFE as part of this work. The VAPSHCS Center for Limb Loss and MoBility shall provide performance data without identifiers (i.e., GFI) to enable Tasks.

## Other Pertinent Information or Special Considerations.

Special considerations necessary to accomplish the contract include significant experience directing extramural research projects funded by National Institutes of Health, Department of Veterans Affairs, or the National Science Foundation, to develop musculoskeletal models and human movement simulations. Relevant research projects include work to gain insight into the biomechanics and neuromotor control of human movement.

a. Identification of Possible Follow-on Work: Not applicable.

b. Identification of Potential Conflicts of Interest (COI): The customer has determined that no organizational COI or other COIs exist.

e. Inspection and Acceptance Criteria: The Contracting Officer’s Representative (COR) will be responsible for technical administration of this contract as shall assure proper Government surveillance of the contractor’s performance. As per the Quality Assurance Surveillance Plan associated with this contract, the COR shall contact/meet with the contractor at least semi-annually to assess performance and shall provide a written assessment. Direct observation and analysis of reports shall be used to monitor performance.

## Risk Control

There will be no human subjects research conducted as part of this contract without institutional review board approval.

## Place of Performance

Work will be performed at the Contractor’s site. Contractor will also deliver the Harmony to VA and appear on site to train VA Researchers. They will provide remote support and troubleshooting within 24 hours. The Contractors may have additional VA site visits for in-person support and troubleshooting within two weeks.

## Delivery Schedule

Delivery of reports and documents supporting completion of all Tasks shall be submitted upon completion, but no later than May 2025 (Base Year) and May 2026 (Option Year 1).

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY language

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.

1. ACCESS to VA INFORMATION AND VA INFORMATION SYSTEMS
2. A contractor/subcontrator 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.
3. 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.
4. 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.
5. 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
6. 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.
7. VA INFORMATION CUSTODIAL Language
8. 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).
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. SECURITY INCIDENT INVESTIGATION
21. 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.
22. 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.
23. 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.
24. 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.
25. LIQUIDATED DAMAGES FOR DATA BREACH
26. 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.
27. 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.
28. Each risk analysis shall address all relevant information concerning the data breach, including the following:
29. Nature of the event (loss, theft, unauthorized access);
30. 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.

1. 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.

1. SECURITY CONTROLS COMPLIANCE TESTING

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. With 10 working-day’s 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. 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.

1. TRAINING
2. 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:
3. 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;
4. Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
5. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
6. 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.]*
7. 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.
8. 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.