

FUNCTIONAL/PERFORMANCE STATEMENT

TRUE DIGITAL RADIOGRAPHY AND FLUOROSCOPY SYSTEM - ONE TIME PURCHASE

A. Performance Specifications:

West Texas VA Healthcare System, Radiology Service, requires a onetime purchase for a True Digital Radiography & Fluoroscopy system equal or better to the Siemens Luminos Agile system- Shall include all hardware, software and accessories to perform fluoroscopy (barium enema, barium swallow, modified barium swallow, upper GI), general radiology procedures (chest, abdomen, spines, extremities) and integrate with existing digital video recording module for FEES digital recorder. System shall fit in existing radiology room without major modifications.

Equipment Requirements: equal or greater to the EZ PIC universal package (video acquisition workstation), one (1) 17"x17" flat panel detector for dynamic and static imaging, height adjusting table with a minimum of 26" and maximum of 44", (Fluoro table height of 32"), table weight capacity of 600lbs with a minimum 23" opening for larger patients, table tilt 90/20, one (1) wireless detector with wall stand with comprehensive dose reduction (wireless detector shall have auto tracking of tube and detector), clip on grid for portable detectors, lateral detector holder, two (2) transparent grid (one 15/80- F115 and 115/80- F180), fully motorized detector movement in tower, 19" high contrast flatscreen monitor on a mobile display trolley, 80 kW with 100 kV IEC 60601-2-7 100MA at 79kV x-ray generator, DICOM query retrieve, worklist, print and store for Vista Imaging or other commercial PACS, capability to download images directly to CD/DVD, integrate with existing digital video recording module for FEES digital recorder, radiolucent table pad, monitor and computer system display shall be HIPPA compliant, capability to perform remote diagnostic services, one (1) year warranty with service and technical support along with an additional one (1) year full service maintenance contract (2nd yr), 24 hrs offset training for 1 technologist, 24 hrs initial onsite training and 36 hrs of follow up training to be provided within 90 days after initial training, biomed training tuition, two set of service and operator's manuals.

Trade-in equipment (including de-installation) shall include: Siemens Sireskop Radiography and Fluoroscopy system, Serial# 34115; software WIN NT4 SP6, purchased 4/3/2002

Information Security & Privacy

Information Security & Privacy:

- a. The contractor, their personnel, and their subcontractors shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and information system security as delineated in this contract.

- b. 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.
- c. 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.
- d. 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.
- 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.
- f. 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).
- g. 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.
- h. 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.
- i. 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.
- j. 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.

- k. 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.
- l. Each risk analysis shall address all relevant information concerning the data breach, including the following:
 - i. Nature of the event (loss, theft, unauthorized access);
 - ii. Description of the event, including:
 - 1. date of occurrence;
 - 2. 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;
 - 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.
 - iii. The contractor/subcontractor agrees to comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act.

- m. 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:
 - iii. 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;
 - iv. Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
 - v. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
 - vi. 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.]*
 - 1. 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.
 - 2. 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.
- m. VA sensitive information is to be transferred between the audiology device and VISTA only through the use of a serial Data Innovations panel will not go outside the VA network or information system.