U.S. Department of Veterans Affairs
Answer to Questions for the Record
"VA Electronic Health Record Modernization: The Beginning of the Beginning"
Committee on Veterans' Affairs
U.S. House of Representatives

August 1, 2018

Congresswoman Julia Brownley

QUESTION 1. "During the June 26, 2018 full Committee hearing, VA indicated that it had various enforcement abilities to compel private electronic health record companies to participate in increased data sharing between the VA and community providers, in order to promote interoperability. Please detail for the Committee what those enforcement tools are."

VA Response: VA's enforcement tools center around the use of contracts. In the contract with Cerner Corporation, VA specified the use of the CommonWell service to act as a Health Information Exchange (HIE) between VA/DoD and participating community providers that operate on multiple different platforms to enable clinical data sharing. Additionally, VA has structured contracts with community providers to include preferred data standards and transactional elements. VA tools to promote interoperability are supplemented by the national interoperability drivers in Centers for Medicare & Medicaid Services (CMS) and Office of the National Coordinator for Health Information Technology (ONC).

Congressman Scott Peters

To Acting VA Secretary O'Rourke or Mr. Short:

QUESTION 2. The VA has announced its intent to move to a cloud based system, if so:

a. **How is the infrastructure and architecture being supported?**

VA Response: VA has implemented a secure, cloud-based infrastructure and architecture through the creation of the VA Enterprise Cloud (VAEC), a multi-vendor platform for the development and deployment of VA cloud applications. The VAEC is built on top of two leading cloud service providers (CSPs)—Amazon Web Services (AWS) Government Cloud and Microsoft Azure Government (MAG)—both of which are government-only cloud platforms. Both AWS and MAG have met stringent federal security requirements including the High Baseline Requirements under the Federal Risk and Authorization Management Program (FedRAMP). In the future, the VAEC can be expanded to include other cloud platforms.

The VAEC architecture is also designed to support the rapid rollout of cloud-based applications. For example, part of the VAEC architecture includes a toolkit of common, general support services (GSS) which includes capabilities such as user/access authentication and performance monitoring which each application can leverage, speeding and simplifying the migration of existing or development of new applications in the cloud. The VAEC also implements many of the National Institute of Standards and Technology (NIST), FedRAMP and VA-required privacy and security controls reducing the time each application should take to obtain a VA Authority to Operate (ATO).

b. What security strategy is being used to implement a security system to secure the data in the cloud?

VA Response: The VAEC Cloud Security Strategy ensures Veteran data is secure by leveraging FedRAMP-authorized solutions. The VAEC implements data safeguards through a layered approach including:

i. encrypted data transfer,
ii. encryption at rest within the VAEC GovCloud instances,
iii. role-based access controls,
iv. industry best practice security scanning solutions,
v. audit controls with the CSP for access violations (such as unregistered systems and gateways), and
vi. password policies.

All VAEC government-focused clouds including AWS and MAG are restricted to government agency use. For security controls under Agency responsibility, VA follows OMB- and National Institute of Standards and Technology (NIST) mandated guidance. Additionally, all interconnections between the CSPs and VA use dedicated, government-managed, trusted network connections which are encrypted following federal guidelines. Data security is of paramount importance to VA.

This Cloud Security Strategy uses the VA Enterprise Security Architecture (ESA) Framework that is based on the National Security Agency (NSA) Community Gold Standard Framework Version 2.0. The VA ESA Framework includes four overarching cybersecurity functions: Govern, Protect, Detect, and Respond & Recover. Each function defines cybersecurity capabilities and activities to adequately secure VA's cloud environment. The VA ESA Framework follows and aligns with the NIST Cybersecurity Framework.

VA uses an incremental approach that continuously evolve the required cloud security functions, capabilities, and solutions to address risks and support VA business and IT initiatives. The implementation of each capability requires a three-pronged approach that involves people, processes and technologies. For each capability, VA identifies and assess technologies that can improve the security and resilience of the VA cloud environment.

QUESTION 3: Will the VA continue to support consolidation of its IT footprint to reduce cost? What will Cerner's role be to support this effort as a new prime contractor?

VA Response: The VA Office of Information Technology (OIT) is ultimately responsible for managing VA's IT footprint. The Office of Electronic Health Record Modernization (OEHRM) only has a small portion of VA's IT footprint focused on the EHR modernization effort. OEHRM and OIT look forward to collaborating on future acquisitions to ensure a judicious use of resources in support of our Veterans. The terms and conditions of the Cerner EHR contract call for a replacement, transition, integration, and/or interfacing of existing systems in support of maintaining the continuity of care to our Veterans and other beneficiaries through an electronic health record. During FY19, VA will be developing a "pivot" strategy in support or the transition of legacy VistA EHR systems to the new Cerner Millennium solution.

QUESTION 4: What steps are being taken now to ensure no PII (personally identifiable information) or medical data is being lost or stolen?

VA Response: VA protects PII or medical data against loss of theft as follows:

1. Completion of a Privacy Threshold Analysis (PTA) and Privacy Impact Analysis (PIA). The purpose of the PTA/ PIA is to: (1) ensure handling of information conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

2. Any VA PII or medical data stored in the cloud must be FedRAMP certified at the High level which would enable VA to rapidly adapt from old legacy systems to secure and cost-effective cloud-based technology. FedRAMP certification aligns with the NIST Risk Management Framework covered in NIST SP 800-37. Higher security levels have a higher level of authentication required in order to enter, access, and gain control of these systems resulting in tighter security to protect VA PII and medical data.

3. The Interconnection Security Agreement and Memorandum of Understanding (ISA/MOU) have been executed. VA utilizes this to document the terms and conditions for sharing VA data by connecting systems in a secure manner and identify and address any security and privacy risks.

4. The contractors involved in the implementation and management of Cerner Millennium are required to complete training on the privacy and security of protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) regulations, as well as the Information Security training, which contains the Rules of Behavior (ROB) they must sign, acknowledging their responsibilities to protect PHI.

To Acting Secretary VA O'Rourke:

QUESTION 5: What is the status of hiring health IT staff needed for this project?

VA Response: The Department of Veterans Affairs (VA) is working through the classification process with Human Resources Management and Consulting Service. Specifically, VA is finalizing position descriptions for health information technology (IT) positions needed for the Office of Electronic Health Record Modernization (OEHRM) and will then begin the recruitment process. VA plans to hold typical recruitment activities, including career fairs, and plans to utilize direct hire authority for the GS-2210 positions to attract qualified talent.

a. Is the VA having trouble finding people who have the experience necessary to execute this project?

VA Response: VA does not believe it will have trouble finding staff with the appropriate knowledge, skills, and abilities once OEHRM is able to directly hire staff. OEHRM is currently working with Human Resources Management and Consulting Service to classify government position descriptions and in the interim, OEHRM is supplementing with the Project Management Office's (PMO) contracted support to fill critical vacancies as a temporary solution. OEHRM will also be able to hire industry experts via the Intergovernmental Personnel Act (IPA) to ensure the program has the necessary clinical expertise and electronic health record (EHR) deployment experience.

b. Can our Committee assist in any way to attract talented people to make sure this project is successful?

VA Response: VA sincerely appreciates the offer for assistance and believes that if provided with the appropriate level of funding and oversight, this program will be highly successful and ultimately provide better care for our Nation's Veterans. VA will continue to engage with Congress on ways that we can together work to ensure that VA can attract and retain the most talented professionals in their fields to contribute to the mission of serving Veterans.