Congress of the United States
Washington, DC 20515

December 2, 2011

Dr. Jonathan Woodson
Director
TRICARE Management Authority
Skyline 5, Suite 810, 5111 Leesburg Pike
Falls Church, VA 22041-3206

Dear Dr. Woodson:

We are writing to express our deep concerns about a major breach of personally identifiable and protected health information (PII/PHI) by TRICARE Management Authority (TMA) contractor Science Applications International Corporation (SAIC). This breach resulted in the loss of names, Social Security Numbers, addresses, dates of birth, phone numbers, provider information, and laboratory tests belonging to 4.9 million military clinic and hospital patients. This breach by a firm responsible for handling the military health provider's patient data represents an extremely serious and substantial lapse in security.

According to the SAIC notification provided to patients impacted by the breach, a company employee reported that computer backup tapes containing patient data were stolen from his vehicle in San Antonio, Texas (see attached SAIC notifications). The notification goes on to explain that the use of these backup tapes and the method of transporting them are "routine procedure" for the company. According to reports, the tapes were left in the vehicle for most of the day and included specific information regarding patient diagnoses and treatment. This incident raises a number of important issues; accordingly, we request your responses to the questions that follow.

1) What security precautions and protections does TMA require SAIC or other technology contractors to utilize in the handling of patients' PII/PHI?

2) Does TMA require SAIC or other contractors to have a formal documented policy that requires PII/PHI to be encrypted or otherwise be made indecipherable to unauthorized individuals? If yes, please provide a copy of this policy and explain how TMA monitors and enforces compliance with such a policy. If not, why not?

3) Was the handling of the backup tapes a violation of SAIC policy or TRICARE contract requirements for handling sensitive information?

4) Does TMA require SAIC or other contactors to have a formal policy on guidance/restrictions when SAIC employees take PII/PHI off premises? If not, please explain why. If so, please provide a copy of any documents that detail the procedures that are supposed to be followed during such transfers.

5) Does TMA require SAIC or other contractors to perform background checks or provide training of all personnel with access to PHI on the policies mentioned above, as well as HIPAA? Please provide copies of these training materials if such training is mandated by TMA. When was the employee involved in this incident last trained and what did the training entail?

6) Were the computer backup tapes involved in this incident encrypted? If not, please explain why. If so, what encryption algorithm was used and how was the key protected? Was the key in the employee's possession?

7) Did the computer backup tapes contain mental health, addiction, genetic, or other sensitive information?

8) Were patients whose data was breached seen at particular hospitals or by certain providers? Were there particular subgroups affected out of the 10 million TRICARE beneficiaries (e.g., patients from specific geographic regions)? If yes, which ones?

9) According to a September 2011 report by PwC's Health Research Institute "Old Data Learns New Tricks," the problem of medical identify theft is worsening as electronic sharing of patient data increases. Medical identity theft, which the report identifies as the fastest growing form of identity theft, occurs when scam artists seek services under another person's name. The victim is often left with huge medical bills, damaged credit, and erroneous medical records.[1]

   While SAIC has offered to provide victims of this most recent data breach with credit monitoring services for a year, such services are useless in protecting against medical identity theft and fraudulent health insurance claims. Will TRICARE require SAIC to provide victims with newly available medical identity theft monitoring? If not, please explain why not.

This is not the first time that sensitive data has been breached while under SAIC's control. In fact, SAIC has had at least six prior security incidents due to malware infections, stolen computers, and, last year, stolen computer backup tapes. For example:

- On June 30, 2010, SAIC notified the Maryland Office of the Attorney General that it had discovered a "theft of backup tapes" that may have exposed personal information including Social Security numbers (see attached SAIC notifications).

- On January 1, 2008, SAIC notified the Office of the Massachusetts Attorney General that malware had infected a company computer and, as a result, the credit card information of certain customers was potentially compromised (see attached SAIC notifications).

---

[1] "Old Data Learns New Tricks." PwC Health Research Institute, Sept. 2011.

- On July 20, 2007, SAIC announced that the Social Security numbers and personal health records (in the form of codes) of nearly 900,000 troops, family members, and other government employees stored on a non-secure computer server were compromised because SAIC did not encrypt data it sent online.[2]

- On February 12, 2005, SAIC notified 45,000 past and present employees – including top military and intelligence officials – that they were at risk of identity theft after computers containing Social Security numbers, financial transaction records, and other personal information were stolen during a break-in at their San Diego administrative building.[3]

In light of these incidents, we are interested to learn what steps TMA has taken since these breaches - and what future action will occur – to prevent additional data leakage. Specifically:

10) Was TMA aware of SAIC's prior data breaches before awarding this contract?

11) If TMA was aware of SAIC's history of data breaches, were additional safety precautions included in the contract to mitigate the risks of another breach? If not, why not?

12) Is SAIC's information security system independently certified by the Federal Information Security Management Act (FISMA)? If it is not FISMA certified, please explain why not. If it is, please provide a copy of the audit report.

13) This latest breach appears to be at least the second incident involving the theft of SAIC's computer backup tapes. The SAIC notification letter stipulates that SAIC was obligated by its contract with TMA to transfer the backup tapes to a secure location. Is this accurate? Given the option of storing backup tapes via other means that do not require physical transport (e.g., on secure servers through cloud computing), why did TMA require physical transport?

14) Going forward, will TMA require SAIC and its other contractors to eliminate the physical transport of PII/PHI backup tapes in favor of a more secure and reliable method? If yes, which ones? If not, why not?

15) Since SAIC had previous malware incidents, what policies for scanning and independent penetration testing has the firm implemented to mitigate reduce the risk of future security incidents?

---

[2] McMichael, William. "Data Security Lapse Affects Almost 900,000 - Army News | News from Afghanistan & Iraq - Army Times." *ArmyTimes*. 20 July 2007.

[3] Witte, Griff. "Break-In At SAIC Risks ID Theft." *Washington Post* 12 Feb. 2005.

16) For the past ten years, please list all instances in which PII/PHI has been temporarily or permanently lost, stolen or otherwise gone unaccounted for by TMA or any of its technology contractors engaged in TMA's health care operations.

    For each such instance, please list (a) the date; (b) the contractor or subcontractor as applicable; (c) the type and quantity of PII/PHI involved; (d) the length of time it took to notify individuals about the breach; (e) the resolution of each breach, as applicable; and (f) whether TMA became aware of any unauthorized use of the PII/PHI that may have occurred as a result of the breach (and if so please fully describe such use).

SAIC has received more than $20 billion in federal contracts over the previous three fiscal years, according to USAspending.gov. This is despite the fact that federal officials have lodged complaints against the company's conduct for years.

- In 2005, SAIC faced government charges that it padded its cost estimates on a $24 million Air Force contract. SAIC later agreed to settle the lawsuit for $2.5 million.[4]

- Also in 2005, then-FBI Director Robert Mueller testified before Congress that the company had "botched an attempt to build software for the bureau's new Virtual Case File system."[5]

- In response to the February 12, 2005 breach involving present and past SAIC employee data, David Kay, who served as chief weapons inspector in Iraq after working for years as an executive with SAIC, was quoted by the Washington Post as saying, "I find it unexplainable how anyone could be so casual with such vital information....It's probably just random luck. But multiple occurrences of bad luck are often more than bad luck."[6]

17) Why does TMA continue to contract with SAIC for its data handling and IT needs despite these major performance problems?

In light of the massive scope of the SAIC data breach, we appreciate your timely and thorough response to these questions no later than February 2, 2012. If you have any questions, please contact Sara Schaumburg at 202-225-2836 or sara.schaumburg@mail.house.gov.

Sincerely,

Edward J. Markey
Member of Congress

Joe Barton
Member of Congress

[4] Witte, Griff. "SAIC Settles Allegations Of Defrauding Air Force." *Washington Post*. 28 Apr. 2005
[5] Witte, Griff. "Break-In At SAIC Risks ID Theft." *Washington Post* 12 Feb. 2005.
[6] Ibid.

Diana DeGette
Member of Congress

Cliff Stearns
Member of Congress

Robert Andrews
Member of Congress