Congress of the United States
Washington, DC 20515

May 7, 2012

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

Dear Dr. Woodson:

TRICARE's response to our letter dated December 2, 2011 regarding the data breach involving its contractor, Science Applications International Corporation (SAIC), fails to address many of our concerns. In fact, it raises a number of additional significant questions about the TRICARE's ability to protect the health privacy of members of our military. Protection of the personal health information of our men and women serving in the military is not only a privacy issue. It is a national security imperative. We remain deeply concerned that TRICARE is not adequately safeguarding this sensitive information, to the detriment of millions of service members and their families. Accordingly, we call on TRICARE to promptly implement major, meaningful reforms to ensure the security of the personal health information it collects, maintains and manages on behalf of those who serve in the Armed Forces.

In our letter, we asked for specific assurances about TRICARE's efforts to ensure that its contractors, including SAIC, will avoid the lapses that led to the theft of health records of 4.9 million beneficiaries. It is not clear, based on TRICARE's response, that sufficient changes are underway.

At a minimum, TRICARE should require that its contractors, including SAIC, encrypt data before transporting it to a different location. Yet even after experiencing multiple instances of physical data theft as outlined in our December 2nd letter, TRICARE still does not mandate that its contractors handling sensitive information implement such a commonsense risk mitigation practice.[1] This is unacceptable.

---

[1] Encryption of stored personally identifiable information (PII) is a standard requirement for businesses. Federal Trade Commission "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf, at 24-26 (noting encryption as a means of reasonable security for consumer data); *id.* at 31 (advocating as an additional means of implementing the substantive privacy by design protections, the use of privacy-enhancing technologies– such as encryption and anonymization tools); *id.* at 33 (noting by example the proliferate collection and storage of unencrypted data as a reason for improved collection, storage and security protocols)

PRINTED ON RECYCLED PAPER

In its response, TRICARE blames its failure to encrypt sensitive data on outdated technology incapable of providing such protection. The response states that encrypting the data involved in the most recent breach requires "careful thought and detailed guidelines…In this case, while some of the components were encrypted, not all of the data contained on the computer backup tapes were capable of FIPs-compliant encryption due to the technical challenges associated with older applications." In other words, it appears that TRICARE blames its lack of adequate security protections on a "legacy" (i.e. outdated) system with "no available technical solution for encryption" to meet federal standards. Such limitations do not excuse TRICARE's and its contractor's lax treatment of such sensitive data.

Despite the fact that this is at least the second incident involving the theft of SAIC's computer backup tapes, TRICARE has still not abandoned the physical transport of such data in favor of electronic transmission over a secure virtual private network (VPN). TRICARE states that "[a]ctions and studies are underway" to look at this issue, but "no such decision has been made at this time." With SAIC's history of serious security failures, it is disturbing that TRICARE engaged this contractor for such sensitive work. Given SAIC's past security breaches, it seems it would have been helpful for TRICARE to perform spot checks or verification that contractors were complying with training and the Business Associate Agreement. TRICARE's response to our letter failed to indicate whether it conducted any of those activities.

We also found TRICARE's response to our questions about the specific security precautions it requires its contractors to implement in handling personal health information to be vague and incomplete. Specifically, TRICARE stated that such protection "is governed and implemented through statute, regulation, and policy. The three primary statutes that protect PII/PHI are the Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA) with its implementing Privacy and Security Rules, and the Health Information Technology for Economic and Clinical Health (HITECH) Act". Mere recitation that contractors are "required to comply with applicable DoD regulations, policies, and instructions" along with data sharing agreements does not demonstrate that TRICARE is taking the necessary action to protect the security of our military's records.[2] In fact, the lack of specific information raises further questions about the extent to which TRICARE follows these important statutes.

Since sending our original letter in December, it has come to our attention that some TRICARE beneficiaries whose information was breached by SAIC have been subject to identity theft, which they attribute to this data breach. For example, Carol Keller, the Revere, Massachusetts and wife of a disabled Air Force veteran, has experienced multiple fraudulent charges against her credit card after her personal information was disclosed in the breach.

---

[2] TRICARE claims a DOJ Certification without identifying if this is annual or performed by a third-party security auditor. Nor does TRICARE identify any compliance results, if such results even exist.

Some victims have had to pay out of pocket for credit monitoring services because TRICARE and SAIC refused to provide these services to victims of the breach until after the victims sued TRICARE and SAIC. Others have had to pay for medical identity protection, which TRICARE and SAIC still refuse to provide to victims of the breach. TRICARE claims the remedies offered are adequate because its policies "hold beneficiaries harmless in the extremely unlikely case that a third-party would seek to use the type of information found here to file a fraudulent claim," but this does not protect them from alteration of their medical records, a fraudulent activity that is incredibly time-consuming stressful for victims to resolve. The men and women who serve our country deserve much better.

We appreciate TRICARE's offer to provide a briefing on this issue, and we look forward to addressing these concerns. In the meantime, we call on the agency to take the steps necessary to ensure that both TRICARE and its contractors uphold the standard necessary to ensure the health privacy of our service members and their families. If you have any further questions, please contact Sara Schaumburg in Congressman Markey's office at sara.schaumburg@mail.house.gov or 202-225-2836 or Emmanual Guillory in Congressman Barton's office at emmanual.guillory@mail.house.gov or 202-225-2002.

Sincerely,

Edward J. Markey
Member of Congress

Joe Barton
Member of Congress

Robert Andrews
Member of Congress

Cliff Stearns
Member of Congress