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

The protection of Personally Identifiable Information (PII) and Protected Health Information (PHI) within the Department of Defense (DoD) is governed and implemented through statute, regulation, and policy. The three primary statutes that protect PII/PHI are the Privacy Act of 1974, as amended (Privacy Act), 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, which was enacted as part of the 2009 American Recovery and Reinvestment Act. Contractors, including SAIC, that access DoD information systems containing PII/PHI are contractually required to comply with applicable DoD regulations, policies, and instructions.

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?

No, TMA does not require contractors to have a formal policy implementing encryption requirements. In the case of the SAIC contract, while not considered contractual documents, as noted in Response #1 above, there is a required privacy act assessment (PIA) and a data sharing agreement (DSA) on file. The primary system involved is a legacy system with no available technical solution for encryption that meets Federal Information Processing (FIPS) standards.

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

The contractor’s performance of the statement of work requirements in Contract W74V8H-04-D-0036, Task Order (TO) 0030 includes a Business Associate Agreement required by HIPAA. As such, the incorporation of a BAA into the aforementioned contract served as (one of multiple) SAIC’s contractual requirements and agreement to abide by and comply with HIPAA, Privacy and Security regulations in accordance with the terms and conditions of the BAA. Specifically, the BAA states,

> “The Contractor shall use appropriate safeguards to prevent use or disclosure of the Protected Health Information (PHI) other than as provided for by this Contract,” and “the Contractor shall use administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits in the execution of this contract.”

Numerous additional contractual requirements relating to the safeguarding and protection of PII/PHI are identified throughout TO 0030. In addition to the SAIC’s agreement to comply with the aforementioned BAA, numerous contractual controls required the contractor to conform to strict and extensive protections for PHI, PII, and Sensitive Information, required by policies and procedures in accordance with Federal, DoD, and MHS mandates to ensure the security of systems, data and other media with 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.

See Response #3. With respect to this specific incident the tapes are stored at the Military Heath System (MHS) Enclave in San Antonio (MESA) a GSA-leased commercial facility that provides a secure location for electronic data in case of a catastrophic event on a military installation. Pertinent parts of the policies which pertain to the MESA site are at enclosure (1).

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?

Yes, the TMA Personnel Security Division (PSD) ensures all contractor employees who manage, design, develop, operate or access DoD Automated Information Systems (AIS) or DoD network systems have the appropriate background investigations. Additionally, PSD conducts "Trustworthiness Determinations" on all contractor employees who hold Automated Data Processing/Information Technology (ADP/IT) positions that directly or indirectly affect the operation of unclassified IT resources and systems that process sensitive but unclassified (SBU) information. Additionally, an interim determination is made regarding a contractor employees' suitability for public trust positions and issuance of a Common Access Card (CAC). As noted in the DSA mentioned above, all users with access to the data on the system in question have appropriate ADP/IT clearances and training commensurate with their level of usage/access.

With regards to training requirements, TMA currently requires contracts to contain language requiring contractors to complete HIPAA Privacy and Security training and IA training. The employee involved in this incident completed the required training. Enclosure (2) provides a copy of the TMA's training material for Information Assurance Annual Training. Enclosure (3) provides a copy of TMA's Privacy Act and HIPAA Annual Training.

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?

No. DoD issued a policy memorandum on encryption on March 19, 2008. That policy does not mandate encryption of unclassified data on removable storage devices used to backup data on networks or servers that are stored for prescribed periods of time, whether those devices are thumb drives, CDs, hard disks, tape drives, etc. Encrypting backup media requires careful thought and detailed guidelines since it introduces several management and configuration control issues especially if the media is stored for many years. 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 clinical applications such as Composite Health Care System (CHCS), the MHS' legacy electronic medical system. Due to the legacy nature of CHCS' software, where there is no FIPS-compliant software, the development, testing and implementation of encryption software for backup tapes had to be completed, and an ongoing evaluation is now being conducted to ensure encryption at the highest level feasible.

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

Clinical mental health notes are maintained separately and were not included on these backup tapes. The computer backup tapes may have included behavioral health information, addiction information (prescriptions or clinical drug/alcohol tests), results of Commander-directed blood/alcohol tests, and results from genetic and other sensitive laboratory testing.

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?

The PII/PHI at risk of compromise as a result of this breach affects approximately 4.9 million patients in the direct care system. These patients either received care from 1992 through September 7, 2011, in San Antonio area military treatment facilities (MTFs), including the filling of pharmacy prescriptions, or had laboratory workups processed in these same MTFs even though these patients were receiving treatment elsewhere. Data on patients outside of the San Antonio area are included in the backup tapes as a result of the use of Laboratory Interoperability software through which laboratory specimens from other DoD MTFs were submitted to Wilford Hall Air Force Medical Center as the referral laboratory.

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.

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.

TMA (which administers the TRICARE statutory health benefit) will not provide medical identity theft monitoring. TMA already has protections in place which operate to hold TMA and our 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.

TMA directed SAIC to provide a year of free credit monitoring for those who request the service and identity restoration services for individuals who qualify for the service. Each affected individual is being offered twelve months from the date of the notification letter to sign up for the following services and access to the items listed below each:

- Enhanced Identity Theft Consultation and Restoration.
  - Licensed Investigators who understand the problems surrounding identity theft are available to answer questions and offer their expertise regarding any concerns that may arise.
  - A Licensed Investigator will work to help restore an individual’s identity to pre-theft status if their name and credit is affected by the incident.

- Continuous Credit Monitoring.
  - Monitoring alerts make individuals aware of key changes, using data from their Experian credit file that could indicate the kind of unauthorized activity commonly associated with identity theft and fraud.

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

The most notable incident involving the MHS and SAIC was a 2007 data breach and certain TMA personnel were aware of that prior data breach when TO 0030 was placed.

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

See above Responses concerning contract and program requirements.

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.

The information system that served as the source system for the lost backup tapes is a DoD system – not an SAIC information security system.

The DoD system meets the requirements of the DoD Information Assurance (IA) program as prescribed by DoD Directive 8500.01E, “Information Assurance (IA),” October 24, 2002 and DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003. The system has been certified and accredited in accordance with DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” November 28, 2007. The system is compliant with the reporting requirements of FISMA.

13) This latest breach appears to be at least the second incident involving the theft of SAIC's computer backup tapes. The SAlC 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?

SAIC was obligated by its contract to transport the back-up tapes to a secure location. TMA requires the back-up of data so that it can continue operations in the event of a catastrophic systems failure caused by external or internal forces. Back-up tapes have historically been used for this purpose and were used in this instance.

Typically, CHCS is operated on military installations and backup tapes are moved securely within the same installation. This is not the case with respect to this specific incident wherein the tapes are stored at MESA, which is unique to the MHS. MESA is a GSA-leased commercial facility, not on an installation, that provides a secure location for electronic data in case of a catastrophic event on a military installation. Therefore, backup tapes were moved between MESA and the U.S. Army Medical Information Technology Center (USAMITC) located on Fort Sam Houston, Texas, a total distance of less than 10 miles.

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?

Actions and studies are underway to enable electronic transmission of tape backups over a secure virtual private network (VPN) from each site to a secure, centrally located server approved by the government, thus eliminating the need for physical transport to offsite storage. However, no such decision has been made at this time.

To the extent that physical transport continues to be required, TMA will only permit the movement of tapes that are encrypted.

Additionally, TMA awarded a contract on January 3, 2012, for the transport and secure storage of encrypted backup tapes from the MESA facility. However, since this incident, movement of backup tapes from the MESA facility has not commenced. Movement will commence once necessary policies and procedures are in place.

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

The incident at MESA was not related to malware, and we are not aware of any malware associated with DoD applications supported by SAIC.

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).

The DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, defines a breach as the “actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected.”
All breaches involving PII/PHI of MHS beneficiaries are reported to the TMA Privacy and Civil Liberties Office. Since the requirement to report breaches was effective, May 14, 2007, TMA’s records on reported breaches began at that time (late 2007). Below is the best available information concerning breaches that involve technology contractors:

#	Date of Incident	Contractor	Data Elements	Description of Incident	Notification Time w/in 10 Days?	Resolution and Mitigation	Further Unauthorized Use
1	12/7/07	TRO North – Health Net	PHI/PII	Stolen laptop	No, notification took place within 15 days due to the large number affected, 42,000	None provided	No
2	01/10/08	TRICARE Online	PII *(no PHI)*	System allowed viewing of another individual’s PII	Yes. 9 affected	Necessary system configurations were made to prevent any future occurrences.	No
3	07/25/10	Wisconsin Physician Services	PHI/PII	66 accounts were created by the same IP address in the Philippines	Yes. 66 affected	All accounts were deactivated/ Breach investigated by Program Integrity, and HHS/OCR.	No
4	09/14/11	SAIC	PII/PHI, including: Name, SSN, Address, Diagnosis, Treatment Info, Provider Info	A box of 25 backup tapes from CHCS was stolen from an SAIC employee’s vehicle.	No. Due to 4.9 million affected individuals individual notification did not occur within 10 days. Individual notification has since been completed using all known addresses. A substitute notice	Incident reported to police, Congress, HHS/OCR. Credit monitoring offered.	No

					was posted within the 10 day requirement.		

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

Acquisition decisions are made based on best value to the government through full and open or fair opportunity contracting. SAIC contract awards have followed all appropriate acquisition guidelines. Of note, SAIC is one of a limited number of contractors with the requisite skills and knowledge-base capable of performing the complex tasks associated with sustaining and maintaining the expansive network of systems associated with MHS' legacy CHCS and the AHLTA (the Military electronic health record).