OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

TRICARE
MANAGEMENT
ACTIVITY

[Name]
[Street Address]
[City, STATE] [Zip Code]

Dear [Insert Beneficiary Name]:

This letter is to notify you of the potential compromise of personally identifiable information and/or protected health information (PII/PHI) belonging to you, or one or more members of your household. The data elements that may have been compromised consist of the following: your name, Social Security Number, sponsor's Social Security Number (if you are not the sponsor), date of birth, patient name, type of medical specialty to which referred, number of approved visits, referrer, enrollment status, and facility to which referred.

TRICARE Management Activity (TMA) learned of this potential compromise on February 8, 2012, when we were notified by the Defense Information Systems Agency's Global NetOps Support Center that a file containing the above mentioned information was accessed on February 4, 2012 by an unknown IP address overseas. The file consisted of a presentation that was briefed at a 2003 TRICARE Conference, and contained a hidden, embedded spreadsheet of referral patient record fields that included your information. Upon notification, we determined that links to this file had previously been removed from the public web site, but the file remained on the TMA server. Therefore, we immediately removed the file from the server and have confirmed that it is no longer accessible. As of today, we have been unable to determine if, indeed, your information was wrongfully compromised; therefore, we are notifying you of this incident as it is essential that TRICARE beneficiaries remain aware of any events that may affect their privacy. As soon as we learned of the incident, we took steps to identify and locate all of the information embedded within the file, to determine who should receive notification of the incident. Addresses of the individuals became available the second week of March. Other steps taken, in an effort to prevent any future like-occurrences, include TMA review and enhancement of its security policies, implementation of technical solutions to protect data exposure, and strengthening of network operation security business processes. We want you to know TMA continuously reviews the security posture seeking to implement solutions to further enhance our protection of beneficiary information.

TMA deeply regrets any inconvenience this might cause you or any member of your household. We know how concerned you may be, and we desire to provide you with assistance. Therefore, you should be guided by the actions recommended by the Federal Trade Commission (FTC) which can be found at http:www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm. The FTC web site provides information on protecting your identity against fraud, and also provides instructions on placing a free fraud alert on your credit reports for a period of 90 days. Once you

place the fraud alerts on your file, you are entitled to order free copies of your credit reports. Additionally, the site provides other valuable information concerning actions that can be taken now, or in the future, should any problems develop.

We take this potential data compromise very seriously and we continue to strive to protect and secure your information. On behalf of TMA, I apologize for any inconvenience and concern this issue may have caused you.

We look forward to providing further health care management services to you. If you have questions or concerns, please feel free to contact Ms. Linda S. Thomas, Director, TMA Privacy and Civil Liberties Office, at (703) 681-7500 between 8 a.m. and 5 p.m. Eastern Time or via email, at PrivacyMail@tma.osd.mil.

Sincerely,

W. Bryan Gamble, M.D., FACS
Brigadier General, US Army
Deputy Director