

TRICARE.mil PowerPoint Breach Call Script

Q. Is this letter a hoax?

A. No. If you received a letter dated March 22, 2012, signed by the Deputy Director, TRICARE Management Activity (TMA), notifying you of the potential compromise of your personal information, then the letter is valid. The Assistant Secretary of Defense (Health Affairs) directed we notify you of this incident, as it is essential that TRICARE beneficiaries remain aware of any events that may affect their privacy.

Q. What are the details surrounding this incident?

A. TMA learned of the potential compromise on February 8, 2012, when notified by the Defense Information Systems Agency's Global NetOps Support Center that a Power Point used for a briefing at a 2003 TRICARE Conference. The briefing contained hidden, embedded spreadsheets of patient's referral records that included your information, was accessed on February 4, 2012 by an unknown IP address overseas.

Q: Why wasn't I notified sooner?

A. When we were first notified of the incident, we were not sure of the full scope until we worked closely with our Network Operations Division to retrieve and review the files in question. Our comprehensive analysis began with the review of raw data and we didn't know that you were affected by this incident until we completed our analysis and received your name and current address from the Defense Enrollment Eligibility Reporting System on March 6, 2012. At that time, in accordance with DoD regulatory requirements, notification was made within 10 days.

Q. Why was my information available for access by this unknown IP address?

A. The presentation file was intended to be publicly available as a training reference for the Military Health System. The spreadsheet containing your information, along with other beneficiaries - was used to create graphs and charts for the presentation. Although your information was not visibly available on any of the slides within the PowerPoint presentation, it was hidden behind the graphs on an Excel worksheet.

Q. What type of information was contained within the PowerPoint presentation?

A. Personal information may have been compromised consisting 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, referring provider, enrollment status, and facility to which referred. There was no financial data, such as credit card or bank account information, on the spreadsheet.

Q. What is personally identifiable information (PII)?

A. Personally identifiable information or PII is information that identifies, links, relates, or is unique to, or describes an individual. This also includes information that can be used to distinguish or trace an individual's identity and any other personal information that is linked or linkable to a specified individual.

TRICARE.mil PowerPoint Breach Call Script

Q. What is protected health information?

A. Protected health information or PHI is information that is created or received by a covered entity and relates to the past, present, or future physical or mental health of an individual; providing payment for healthcare to an individual; and can be used to identify the individual. It excludes health information in employment records held by a covered entity in its role as employer.

Q. What is the risk to my data? Can just anyone access it?

A. The risk of harm is judged to be moderate since we have no evidence indicating that your information was wrongfully compromised. In addition, retrieving the hidden worksheet requires knowledge of its existence and the skills to uncover the hidden, embedded files and fields.

Q. Has the file been removed?

A. Yes. 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 to the public.

Q. Is anyone investigating this incident?

A. Yes, this incident continues to be under investigation by the Defense Information Systems Agency's Global NetOps Support Center and the Military Health System Cyberinfrastructure Services' Network Operations Branch. We want you to know that we have contained this incident and the file is no longer accessible via TMA's public interfacing web site or server.

Q. What is TMA doing to mitigate this incident and prevent future occurrences?

A. TMA is taking the following actions:

- TMA has reviewed and enhanced security policies, implemented technical solutions to protect data exposure, and strengthened network operation security business processes.
- TMA continuously reviews the security posture seeking to implement solutions to further enhance our protection of beneficiary information.
- TMA is also reviewing all website policies and procedures to improve the safeguards and security controls that are currently in place to ensure personally identifying and/or protected health information is not accessible from any TMA public web server.

Q. What can I do to protect myself?

A. You can monitor your credit reports for any sign of suspicious activity and place a free fraud alert on your credit for a period of 90 days using the Federal Trade Commission's web site. If you detect any suspicious activity, you should report it to the authorities immediately. Tips on how to protect your information are available at:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>

Q. What should I do if I notice suspicious activity on my credit report?

A. Report it to the authorities immediately. Steps that you should take are further described at the Federal Trade Commission's web site:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>.

TRICARE.mil PowerPoint Breach Call Script

Q. What can I do to protect myself against identity theft? What do I do if I believe my identity has been compromised?

A. If you believe your identity has been compromised, you should be guided by the actions recommended by the Federal Trade Commission (FTC) at its web site, which can be found at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm>. This web site provides information about protecting your identity against fraud and placing a fraud alert on your credit report. The free fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new account is opened, a new credit card is issued, or an existing card is changed. The site also provides other valuable information regarding actions that can be taken now or in the future, should problems develop.

Q. How can I obtain a copy of my medical records?

A. You are advised to contact the most recent MTF in which you received healthcare services to obtain copies of your medical records. For additional information on how to go about obtaining your records, please refer to the TMA Privacy Office HIPAA Privacy Information Paper titled “Obtaining Military Records” available at:
<http://www.tricare.mil/tma/privacy/hipaa-privacypapers.aspx>