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

TRICARE
MANAGEMENT
ACTIVITY

NOV 17 2010

MEMORANDUM FOR DIRECTORS, TRICARE MANAGEMENT ACTIVITY

SUBJECT: Updated Guidelines on Protection of Sensitive Information in Electronic Mail

This memorandum updates guidelines in Military Health System Chief Information Officer memorandum "Updated Guidelines on Protection of Sensitive Information in Electronic Mail" of September 19, 2008. Per federal law and Department of Defense (DoD) policy (references attached), all users of the TRICARE Management Activity (TMA)/Health Affairs (HA) network must ensure that sensitive information is protected when transmitted via an e-mail beyond the TMA/HA network. TMA policy requires that any e-mail that contains or has an attachment containing sensitive information and is sent outside the TMA network must be encrypted and digitally signed.

Use of DoD Public Key Infrastructure (PKI) shall always be the primary means to encrypt an e-mail attachment containing sensitive information. If DoD PKI encryption of e-mail attachments is not possible due to business reasons, the attached guidelines provide procedures and products approved for encrypting e-mail attachments containing sensitive information. Products approved for encryption of e-mail attachments are Microsoft Office 2007 or later, WINZIP 11 or later, and Adobe Acrobat 9 or later. It should be noted that DoD PKI is the only approved means to encrypt an e-mail with sensitive information in its text body. All TMA network users are cautioned to review addressees when replying or forwarding an e-mail to determine if it should be encrypted because an addressee is outside the TMA network.

Questions on PKI or these guidelines should be directed to Mr. Daniel Brooks, daniel.brooks@tma.osd.mil, (703) 681-6867, in the Information Assurance Division.

Mary Ann Rockey
Acting Chief Information Officer
Military Health System

Attachment:
As stated

References:

(a) The Privacy Act of 1974, (Public Law 93-579), Title 5 U.S. Code, Section 552a, 2000

(b) Health Insurance Portability and Accountability Act (HIPAA), Security Standards, Title 42 U.S. Code, Section 1306, February 20,2003

(c) Federal Information Security Management Act of 2002 (FISMA), TITLE III -- Information Security, December 2002

(d) Instruction 8520.2, "Public Key and Public Key (PK) Enabling," April 1, 2004

(e) DOD 5200.1 -R, "Information Security Program," January 1997

(f) DOD Directive 5400.1 1 "DoD Privacy Program," May 8, 2007

(g) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

(h) TRICARE Management Activity Memorandum, "Protection of Sensitive Information in Electronic Mail," 13 Aug 2007

(j) TRICARE Management Activity Memorandum, "Updated Guidelines on Protection of Sensitive Information in Electronic Mail," 19 Sep 2008