



REPLY TO  
ATTENTION OF

DEPARTMENT OF THE ARMY  
HEADQUARTERS, UNITED STATES ARMY MEDICAL COMMAND  
2050 WORTH ROAD  
FORT SAM HOUSTON, TEXAS 78234-6013

MCIM

01 FEB 2006

MEMORANDUM FOR

Commanders, US Army Medical Command Major Subordinate Commands  
Directors, OTSG/MEDCOM OneStaff

SUBJECT: Security of Electronic-Mail (e-mail) Containing Electronic Protected Health Information (ePHI)

1. References:

a. Office of The Surgeon General/US Army Medical Command Policy Memo 04-008, MCIM, 18 June 2004, subject: Transmission of Protected Health Information (PHI) Via Electronic-Mail (E-mail).

b. MEDCOM Supplement 1 to Army Regulation 40-66, Medical Record Administration and Health Care Documentation, 11 May 2005.

c. The Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Health Insurance Reform: Security Standards (45 CFR Parts 160, 162, and 164), Federal Register, Vol. 68, No. 34, 20 February 2003.

2. We are concerned about the potential release of ePHI when e-mails are sent without the protections required by the HIPAA Security Rule. The HIPAA Security Rule requires the use of security measures to guard against unauthorized access to ePHI being transmitted over electronic communications networks. Failure to secure e-mails containing ePHI jeopardizes the privacy of our medical information and puts us at risk for the penalties associated with HIPAA.

3. Because there is no single interoperable encryption solution for securing e-mails, policies and procedures have been developed that will either protect or mitigate the security risks to the ePHI being mailed. The following provides a synopsis of these policies:

a. E-mail between users with an "amedd.army.mil" account: Secure ePHI by encrypting the e-mail using the Common Access Card and DoD Public Key certificates as outlined in reference 1a.

b. E-mail between provider and patient: Currently, there is no secure messaging system for e-mail between provider and patient. There are plans to add secure messaging as a feature in TRICARE Online. In the interim, the patient and provider must comply with the requirements outlined in reference 1b. Patients electing to use e-mail for medically related communications

MCIM

SUBJECT: Security of Electronic-Mail (e-mail) Containing Electronic Protected Health Information (ePHI)

must sign a consent form acknowledging the risks of transmitting their PHI through e-mail and authorizing providers to communicate with them via e-mail. The providers will sign a statement of understanding regarding the confidentiality and security requirements for e-mail communications with a patient.

c. E-mail with non-AMEDD organizations: Secure ePHI in an attached, password protected, Microsoft Office file (.doc, .xls, .ppt, etc.). The password should be sent in a separate e-mail. As a reminder, do not send compressed files with the .zip file extension because they will be blocked and discarded by Army's e-mail security system.

4. The security of e-mails containing ePHI must be addressed in your local policies and training programs. In addition, HIPAA requires the imposition of sanctions against members of your workforce who violate these policies and procedures.

5. Our point of contact is Ms. Theora L. Mitchell, Contractor, Office of the Assistant Chief of Staff for Information Management, DSN 471-8347, Commercial (210) 221-8347, e-mail: Theora.Mitchell@amedd.army.mil.

FOR THE COMMANDER:

  
WILLIAM H. THRESHER  
Chief of Staff