TMA Privacy Office Information Paper

E-Mail Encryption

HIPAA Security ♦ September 2012

I. Supporting Regulations and Policies for this Information Paper

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (45 C.F.R. § 164.312(e)(2)(ii)) establishes the requirements affecting e-mail encryption.

B. The "DoD Health Information Security Regulation" (DoD 8580.02-R, C4.6.3.) implements the above part of the HIPAA Security Rule within the Military Health System (MHS).

C. ASD(HA) Memorandum, "Military Health System (MHS) Information Assurance (IA) Policy Guidance and MHS IA Implementation Guides," 23 Feb 2010, provides further policy on e-mail encryption within the MHS.

D. TRICARE Management Activity (TMA) Memorandum, "Updated Guidelines on Protection of Sensitive Information in Electronic Mail," 17 Nov 2010, provides TMA policy and guidance on encryption of e-mail.

II. Guidance for E-Mail Encryption

A. The HIPAA Security Rule requires that TMA, as a covered entity, "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." See 45 CFR § 164.312(e)(i) and DoD 8580.02-R, C4.6.1. The use of encryption is one way to meet this requirement and is an addressable implementation specification (See Information Paper on SPECIFCATIONS: STANDARDS AND IMPLEMENTATIONS).

B. MHS has established policy that all sensitive information (i.e., PHI) sent via e-mail must be encrypted. (See Reference C). This means that TMA workforce members are required to encrypt all emails which contain PHI regardless of whether it's sent to a recipient internal, or external, to the network. PHI is individually identifiable health information maintained by a covered entity and can include such identifiers as names, addresses, telephone numbers, medical records, social security numbers, and other information that could be used to identify an individual. ePHI is PHI that is transmitted or maintained in electronic form.

C. TMA establishes the use of DoD Public Key Infrastructure (PKI) as the only approved means to encrypt e-mail with ePHI in the body of the text, and the primary means to encrypt an e-mail attachment containing ePHI. (See Reference D). If for business purposes, the use of

PKI is not possible, the following products are approved for encryption of e-mail attachments:

1. Microsoft Office 2007 or later
2. WINZIP 11 or later
3. Adobe Acrobat 9 or later

D. It is important to note that password protection is NOT equivalent to encryption. For guidance on using DoD PKI and the alternative approved products, see Enclosure 1 of Reference D.

III. Definitions Associated with E-Mail Encryption

A. Electronic Protected Health Information (ePHI): Individually identifiable health information that is:

1. Transmitted by electronic media; or
2. Maintained in electronic media

B. Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.

C. Public Key Infrastructure (PKI): The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of PK certificates.