PROVIDER ALERT
May 17, 2010

Electronic Protected Health Information (ePHI) in email

The information contained in this provider alert is only intended to be an explanation of how ValueOptions complies with federal security laws. It is not intended to serve as legal advice. If you have questions regarding your company's legal obligations, please seek the advice of an attorney.

Providers and business associates interacting with VO staff should make every effort to keep PHI secure. If your organization does not use email encryption we recommend you send PHI to ValueOptions Maryland through an inquiry in ProviderConnect or by secure fax.

The final HIPAA Security Rule, released in April 2003 and effective April 2005, made the use of **encryption** an addressable implementation specification[i] . Addressable does not mean 'optional', but rather means that if an entity subject to the federal security rule decides that an addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure to meet the standard.

In April 2009 the Department of Health and Human Services (HHS) released guidance that identifies the technologies and methodologies that render protected health information **unusable, unreadable, or indecipherable** to unauthorized users. While entities are not **required** to follow the guidance, the specified technologies and methodologies if used create the functional equivalent of a safe harbor, and thus, result in those entities not being required to provide the notification otherwise required by section 13402 of the HITECH Act in the event of a breach. HHS in consultation with information security experts at the National Institute of Standards and Technology identified two methods for rendering PHI unusable, unreadable, and indecipherable to unauthorized individuals: encryption and destruction.

Guidance released in HHS's interim final regulation on breach notification requirements, published in the August 24 Federal Register, made it clear that though an entity that is not encrypting can be in compliance with the Security Rule (by implementing other safeguards that provide equivalent protection exclusive of encryption) that entity may still be in a position to complete notifications under the HITECH Act if a breach occurs.

Electronic mail sent over the internet is fundamentally insecure. Messages and files sent in plain text (text that is not encrypted) can be intercepted, read, copied and sometimes modified by using traffic monitors or packet sniffers that look for keywords and other content of particular interest.[ii]

ValueOptions® has determined encryption is a reasonable and appropriate safeguard. Encryption at ValueOptions® is used as an access control mechanism in support of HIPAA Security Standard 18: Transmission Security and HIPAA Security Standard 16: Integrity.

[i] 45 CFR §§ 164.312(a)(2)(iv) and 164.312(e)(2)(ii)
[ii] Osterman Research, Inc. The Critical Need for Encrypted Email and File Transfer Solutions. July 2009.