



## Transmission Security Encryption: What to Do and How to Do It

In our series on the HIPAA Administrative Simplification Security Rule, this is the second of two implementation specifications for the Technical Safeguard Standard, Transmission Security. This implementation specification is *addressable*. Addressable does not mean “optional.” Rather, an addressable implementation specification means that a covered entity must use reasonable and appropriate measures to meet the standard. As we noted in earlier postings on HIPAA.com, **business associates of covered entities will be required to comply with the Security Rule safeguard standards, beginning February 17, 2010.** This requirement is one of the HITECH Act provisions of the American Recovery and Reinvestment Act (ARRA), signed by President Obama on February 17, 2009.

### What to Do

Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

### How to Do It

For the sender of electronic protected health information, encryption converts the message in a file or document from a readable to an unreadable format. Decryption is the reverse, allowing encrypted information to be converted from an unreadable format to a readable format by the recipient. **A covered entity should always encrypt electronic protected health information to ensure its integrity and confidentiality.**

As discussed in the earlier posting on the meaning of Transmission Security, a covered entity with only a local network with no electronic connectivity to any person or entity outside of the covered entity may not need to encrypt. With new federal regulations and incentives focused on increasing interoperability amongst healthcare stakeholders, it will be more and more important for these types of covered entities to have encryption capabilities. Any covered entity with open networks should have that encryption capabilities in place now and encrypt all transmissions of electronic protected health information.

**On April 17, 2009, the U.S. Department of Health and Human Services issued *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements* under Section 13402 of Title XI11 (*Health Information Technology for Economic and Clinical Health Act*) of the *American Recovery and Reinvestment Act of 2009*, which is available on the HIPAA.com site. The guidance is related to forthcoming HHS and FTC ‘breach notification’ regulations pertaining to ‘unsecured protected health information.’**

We provide excerpts here from the aforementioned guidance that is germane to electronic protected health information and encryption, therefore to this implementation specification.

“The term ‘unsecured protected health information’ includes PHI [protected health information] in any form that is not secured through the use of a technology or methodology specified in this guidance. This guidance, however addresses methods for rendering PHI in paper or electronic form unusable, unreadable, or indecipherable to unauthorized individuals.

“Data comprising PHI can be vulnerable to a breach in any of the commonly recognized data states: ‘data in motion’ (i.e., data that is moving through a network, including wireless transmission); ‘data at rest’ (i.e., data that resides in databases, file systems, and other structured storage methods); ‘data in use’ (i.e., data in the process of being created, retrieved, updated, or deleted); or ‘data disposed’ (e.g., discarded paper records or recycled electronic media).”

“Encryption is one method of rendering electronic PHI unusable, unreadable, or indecipherable to unauthorized persons. The successful use of encryption depends upon two main features: the strength of the encryption algorithm and the security of the decryption key or process. The specification of encryption methods in this guidance includes the condition that the processes or keys that might enable decryption have not been breached....

“Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

“Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following applies:

“a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by ‘the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key’ and such confidential process or key that might enable decryption has not been breached. Encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

i) “Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End Use Devices*, November 2007. [Available online at <http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf>.]

ii) “Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described in NIST Special Publications

800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005 [Available online at <http://all.net/books/standards/NIST-CSRC/csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf>.];

800-77, *Guide to IPsec VPNs*, December 2005 [Available online at <http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf>.];

800-113, *Guide to SSL VPNs*, July 2008 [Available online at <http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf>]; and

May include others, which are FIPS 140-2 validated.

....”

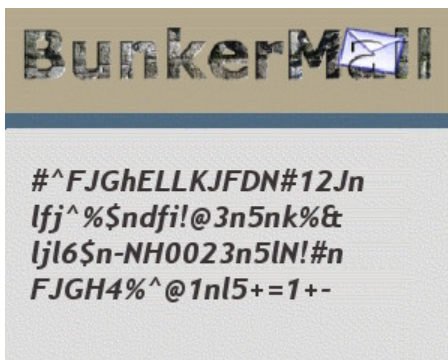
Again, a covered entity must rely on outcomes of its risk analysis to determine whether encryption is necessary. In that risk analysis, the covered entity should evaluate potential risks and costs of breach of unsecured electronic protected health information that becomes accessible to unauthorized users outside of the covered entity, whether data at rest or data in motion, which would trigger the new ‘breach notification’ provisions of the HITECH Act. **If a covered entity does not encrypt electronic protected health information, then it must document its decision and explain why this implementation specification does not apply.** Even in the absence of exposure to an open network, a covered entity should consider in its risk analysis costs and benefits of encrypting electronic protected health information at rest on its closed electronic information system.

With expected increased use of electronic transactions in healthcare, such as e-prescribing, and electronic communications via email, say, between a physician practice and a patient, most covered entities will be using open systems and will have need for encryption tools. HIPAA.com recommends that you contact your electronic information system hardware and software vendors for advice on encryption, and that you also consult the National Institute for Standards and Technology (NIST) Special Publication 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations* (Initial Public Draft), February 2009, [Available online at <http://csrc.nist.gov/publications/drafts/800-53/800-53-rev3-markup-02-05-2009.pdf>], and NIST Special Publication 800-66, Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, October 2008 [Available online at <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf> or for download directly from HIPAA.com].

[Ed Jones](#), Author & Healthcare Authority

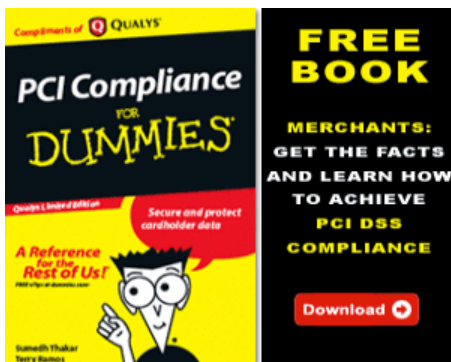
Filed Under: [HIPAA Law: Administrative Simplification](#)

- [HIPAA.com Home](#)
- [About HIPAA.com](#)
- [Our Contributors](#)
- [RSS](#) Syndicate this site
- [✉ Sign up for email updates](#)
- [t Follow HIPAA.com on Twitter](#)



[Advertise on HIPAA.com](#)

- [5010 Version](#)
- [American Recovery and Reinvestment Act](#)
- [Enforcement](#)
- [Health IT and HITECH](#)
- [HIPAA Law: Administrative Simplification](#)
- [Identifiers](#)
- [Meaningful Use](#)
- [Privacy](#)
- [Red Flags Rules](#)
- [Security](#)
- [Transactions & Code Sets](#)



Qualys.com/PCI\_Compliance

Ads by Goooooogle

[Advertise on HIPAA.com](#)

Copyright ©2009 HIPAA LLC | [About HIPAA.com](#) | [Privacy Policy](#) | [Advertise With Us](#) | [Contact Us](#)

⌂ YY