



Approved Encryption and Destruction Methodologies to Render Health Information Secure

Johanna M. Novak

Foster Swift Information Technology News & Foster Swift Health Care Law Report

June 29, 2009

The American Recovery and Reinvestment Act of 2009 (ARRA) contained provisions requiring health care covered entities and business associates regulated by the Health Insurance Portability and Accountability Act (HIPAA) to notify certain parties in the event of a breach of unsecured protected health information (PHI). ARRA defined unsecured PHI as PHI that is not secured through the use of a technology or methodology as specified by Department of Health and Human Service's (DHHS) guidance. Because no such guidance was then in existence, DHHS was quickly charged with the task of meeting with industry stakeholders to determine the appropriate technologies and methodologies acceptable to render PHI stored in any form unusable, unreadable, or indecipherable to unauthorized persons.

On April 17, 2009, DHHS issued this guidance that contained two methods of securing PHI. These methods are the only methods approved by DHHS and are intended to be exhaustive and not illustrative. The guidance can be found [here](#). While covered entities and business associates are not required to adopt the guidance, the specified technologies and methodologies, if used, create the functional equivalent of a safe harbor, and thus, result in covered entities and business associates not being required to provide the notification otherwise required in the event of a breach.

1. Encryption. PHI is rendered unusable, unreadable, or indecipherable to unauthorized persons if electronic information has been encrypted 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.
 - a. Data at Rest. Valid encryption processes for data at rest must be consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

CONTACT

Johanna M. Novak
P: 906.226.5501
E: jnovak@fosterswift.com

AUTHORS/ CONTRIBUTORS

Johanna M. Novak

PRACTICE AREAS

Health Care
Information Technology Law



- b. Data in Motion. 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; 800–77, Guide to IPsec VPNs; or 800–113, Guide to SSL VPNs, and may include others which are FIPS 140–2 validated.
1. Destruction. Alternatively, if the media on which the PHI is stored or recorded has been destroyed in one of the following ways, it is deemed secure:
 - a. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.
 - b. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Ensuring that PHI is secured is important to a health care provider or health insurance company for legal compliance purposes and also for customer service reasons. No provider or insurance company wants to have to notify a patient or insured that their health information was inappropriately released and was unprotected. It will therefore be critical in the next several months for these providers and insurance companies to adopt the DHHS recommendations to fully secure PHI.