# Health Care

## E-ALERT

April 29, 2009

# HHS Issues Guidance and Request for Information on Technologies and Methodologies to Secure Protected Health Information for the Purposes of Breach Notification Provisions

The U.S. Department of Health and Human Services ("HHS") recently has published guidance relating to the Health Information Technology for Economic and Clinical Health ("HITECH") provisions of the American Recovery and Reinvestment Act.[1] Section 13402 of the HITECH Act requires HIPAA covered entities and their business associates to take certain steps to notify affected individuals and HHS following the discovery of a breach of unsecured protected health information ("PHI"). The provision defines "unsecured PHI" to mean PHI that is not secured through the use of a technology or methodology specified by HHS and directs HHS to issue (and annually update) guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. HHS's guidance was effective upon issuance, but will apply to breaches 30 days after publication of forthcoming interim final regulations concerning the breach notification requirement.

HHS states that the guidance is intended to be an exhaustive list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to an unauthorized individual. The guidance also applies to secured personal health record ("PHR") identifiable health information.[2] HHS states that securing PHI with one of the methodologies set forth in the guidance is not a substitute for compliance with HIPAA privacy and security regulations or other federal and state laws; nor should it be considered a substitute for using or disclosing de-identified information when PHI is not necessary to meet the purpose of the use or disclosure.

HHS notes that PHI can be vulnerable to breach in four commonly recognized data states: data in motion (such as data moving through a network); data at rest (data residing in a database or file); data in use (data being created, retrieved, updated, or deleted); and data disposed (discarded or recycled data).

[1] 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 XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009. Office of the Secretary. Department of Health and Human Services. April 17, 2009. www.hhs.gov/ocr/privacy.

[2] The HITECH Act imposes a breach notification requirement on the vendors of PHRs that relates to unsecured PHR identifiable health information. The Federal Trade Commission has recently issued a proposed regulation detailing the breach notification requirements that apply to vendors of PHRs. Health Breach Notification Rule, 74 Fed. Reg. 17914-01 (April 20, 2009) (to be codified at 16 C.F.R. pt. 318).

COVINGTON
COVINGTON & BURLING LLP

BEIJING
BRUSSELS
LONDON
NEW YORK
SAN DIEGO
SAN FRANCISCO
SILICON VALLEY
WASHINGTON

WWW.COV.COM

## I. Methodologies for Securing PHI

According to HHS, there are currently only two methodologies that render PHI unusable, unreadable, or indecipherable—encryption or destruction. HHS also seeks comment on whether data in a limited data set should be considered unusable, unreadable, or indecipherable for purposes of the breach notification requirement.

### A. Encryption

HHS recognizes data as "secured" if it is encrypted with one of the encryption processes that the National Institute of Standards and Technology ("NIST") has judged to "transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."[3] NIST has identified the following encryption processes as meeting this standard:

- Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.[4]
- 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.[5]

### B. Destruction

HHS recognizes data as "secured" if the media on which the PHI is stored or recorded has been destroyed in one of the following ways:

- Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.
- Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*[6], such that the PHI cannot be retrieved.

### C. Limited Data Sets

Limited data sets ("LDS") are PHI from which 16 of the 18 direct identifiers listed at 45 CFR 164.514(e)(2) of the HIPAA Privacy Rule have been removed, but the data may still contain certain dates relating to the individual and certain geographic information so that the data cannot be considered de-identified. Under HIPAA, LDS are still protected due to the risk of re-identification. HIPAA does, however, draw distinctions between PHI in a LDS and PHI that contains direct identifiers. HHS seeks public comment regarding whether data in a LDS should be considered "secured," whether the risk of re-identification of a LDS warrants exclusion from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, and whether a LDS should be considered secured if certain of the remaining indirect identifiers (e.g., month and day of birth, or last 3 digits of a 5-digit zip code) were removed.

[3] 45 CFR 164.304, definition of "encryption."
[4] Available at http://www.csrc.nist.gov/.
[5] Available at http://www.csrc.nist.gov/.
[6] Available at http://www.csrc.nist.gov/.

## II. Opportunity for Comment

In addition to seeking comment on whether data in a LDS should be considered secured, HHS is seeking comment on: other methodologies that should be considered to render PHI (either in electronic or paper format) unusable, unreadable, or indecipherable to unauthorized individuals; on circumstances under which the methodologies identified by HHS as acceptable methods of securing PHI would fail to secure the data; and on whether HHS should identify in its guidance off-the-shelf products that meet the encryption standards. HHS is also seeking comment on the breach notification provision generally, particularly with respect to its interaction with state breach notification laws.

HHS will be accepting comment until May 21, 2009.


If you have any questions concerning the material discussed in this client alert, please contact the following Covington attorneys:

| | | |
|---|---|---|
| Anna Kraus | 202.662.5320 | akraus@cov.com |
| Scott Danzis | 202.662.5209 | sdanzis@cov.com |
| Noellyn Davies | 202.662.5681 | ndavies@cov.com |