



BALCH & BINGHAM LLP

Alabama • Georgia • Mississippi • Washington, D.C.

## HEALTHCARE BULLETIN

*April 24, 2009*

---

### **HHS ISSUES GUIDANCE ON SECURING PROTECTED HEALTH INFORMATION**

---

On April 17, 2009, The Department of Health and Human Services (“HHS”) issued guidance specifying the technologies and methodologies that can be used to secure protected health information (PHI) and to render such information unusable, unreadable or indecipherable to unauthorized individuals. The guidance provides covered entities and their business associates with the means to determine whether there has been a breach of unsecured PHI and whether that breach triggers notification obligations under the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”).

#### Background

The HITECH Act, among other provisions, requires HHS to issue interim final regulations within 180 days after enactment detailing breach notification obligations of entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates. In particular, Section 13402 of the HITECH Act requires HIPAA covered entities to notify affected individuals and potentially the HHS Secretary and the media, and requires business associates to notify covered entities, following the discovery of a breach of “unsecured” PHI.

A breach of unsecured PHI occurs where there is an “unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of that information, except where the unauthorized person to whom the information was disclosed would not reasonably have been able to retain such information.” A breach does not include an unintentional disclosure or use by an employee or individual acting under the authority of the covered entity or the business associate if the disclosure or use was made in good faith. Under the HITECH Act, a covered entity that has discovered a breach of unsecured PHI must notify each individual whose PHI had been accessed, acquired or disclosed in the breach within 60 days after discovery of the breach.



Section 13402(h) of the HITECH Act defines “unsecured protected health information” to mean PHI that is not secured through the use of a technology or methodology required in HHS guidance to render PHI “unusable, unreadable, or indecipherable to unauthorized individuals.” The HITECH Act directed HHS to issue guidance setting forth the required technologies and methodologies by April 18, 2009.

### HHS Guidance

After consulting with information security experts, HHS has identified two methods for securing and rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction. Both of these methods are discussed below.

#### *A. Encryption*

Encryption is one method of rendering electronic PHI unusable, unreadable, or indecipherable to unauthorized individuals. The successful use of encryption depends upon both the strength of the encryption algorithm and the security of the decryption key or process. The following encryption processes have been tested by the National Institute of Standards and Technology (NIST) and are deemed sufficient to satisfy the HHS guidance:

- Encryption processes consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, are valid for data considered to be “at rest” (i.e., data that resides in a database or file system).
- Encryption processes consistent with Federal Information Processing Standards (FIPS) 140-2 are valid for data considered to be “in motion” (i.e., data moving through a network, including wireless transmission).

#### *B. Destruction*

The HHS guidance also addresses the destruction of PHI both in paper and electronic form as a method of rendering such information unusable, unreadable, or indecipherable to unauthorized individuals. PHI in written form will be rendered unusable, unreadable or indecipherable to authorized individuals if the materials have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. PHI in electronic form will be rendered unusable, unreadable or indecipherable to authorized individuals if the information has been cleared, purged or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.



Compliance.

The guidance will apply to breaches 30 days after publication of the forthcoming interim final regulations. While covered entities and business associates are not required to follow the guidance, the two methods, if used, create the functional equivalent of a safe harbor, and thus, result in covered entities, and business associates, not being required to provide breach notification otherwise required by the HITECH Act.

\*\*\*

Should you have any questions, please do not hesitate to contact one of our healthcare attorneys at the offices below.

H E A L T H C A R E C O N T A C T S

**BIRMINGHAM, AL**

Matthew A. Aiken  
205.226.3425  
[maiken@balch.com](mailto:maiken@balch.com)

Colin H. Luke  
205.226.8729  
[cluke@balch.com](mailto:cluke@balch.com)

Jack B. Levy  
205.226.8750  
[jlevy@balch.com](mailto:jlevy@balch.com)

**MONTGOMERY, AL**

Dorman Walker  
334.269.3138  
[dwalker@balch.com](mailto:dwalker@balch.com)

**ATLANTA, GA**

Richard D. Sanders  
404.261.6020  
[rsanders@balch.com](mailto:rsanders@balch.com)

Philip M. Sprinkle, II  
404.261.6020  
[psprinkle@balch.com](mailto:psprinkle@balch.com)

**GULFPORT, MS**

H. Rodger Wilder  
228.214.0412  
[rwilder@balch.com](mailto:rwilder@balch.com)

**JACKSON, MS**

Dinetia Newman  
601.965.8169  
[dnewman@balch.com](mailto:dnewman@balch.com)

The Healthcare Bulletin is published as an informational resource for clients and friends of Balch & Bingham LLP. It does not contain legal advice, and is not a solicitation to perform legal services. No representation is made that the quality of legal services performed by Balch & Bingham LLP is greater than the quality of legal services performed by other lawyers. Design, logo, and content © 2009 Balch & Bingham LLP.

