

# Breach Notification Regulation Addresses PHI Disclosure



By Ann Bachman, MT (ASCP), CLC (AMT)

The Health Information Technology for Economic and Clinical Health (HITECH) provisions of the 2009 American Recovery and Reinvestment Act (ARRA) included Breach Notification Regulations. Written by the Office for Civil Rights, these laws apply to all “covered entities” as defined by the Health Insurance Portability and Accountability Act (HIPAA).

The Regulation defines a “breach” as an impermissible use or disclosure that compromises the security or privacy of unsecured protected health information (PHI) and poses a *significant* risk of financial, reputational, or other harm to the affected person(s). This does not include every impermissible use or disclosure.

## UNSECURED PHI

Notification is required only if the breach involves “unsecured” PHI – PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals by using a technology or methodology specified by the Secretary of the Department of Health and Human Services (HHS).

Acceptable methods of securing PHI include the following:

- Encryption of data at rest that meets the National Institute of Standards and Technology (NIST) Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.
- Encryption for data in motion that complies with the Federal Information Processing Standards.
- Destruction of storage media in one of the following ways:
  - a) Paper, film, or other hard copy that has been shredded

or destroyed so it cannot be read or reconstructed.

- b) Electronic media that has been cleared, purged, or destroyed according to NIST Publication 800-88, *Guidelines for Media Sanitization*, so that information cannot be retrieved.

The Rule allows three exceptions:

- An *unintentional* acquisition, access, or use of the PHI by a member of the workforce acting under the authority of a covered entity or a business associate.
- An inadvertent disclosure of PHI by a person authorized to access the information to another person authorized to access the information *at the same covered entity or business associate*.
- The covered entity or business associate has a good faith belief that the unauthorized individual who received the information was *unable to retain the information*.

## PRACTICE POLICY

Every covered entity, including physician practices, must develop, implement and enforce a practice policy to follow the breach notification regulations. This policy includes staff training, which may be live presentations, web casts and written communications.

When a staff member becomes aware of a breach, he or she must notify the Privacy Officer, who should then investigate the incident, document all findings, and initiate notification processes required if the incident meets the above definition. The

practice must maintain copies of all documentation and notices. Any member of the workforce found violating this or any other HIPAA violation should be dealt with according to the practice’s disciplinary policy.

## INDIVIDUAL NOTICE

When a breach is discovered, the practice must notify each affected individual by first-class mail or, if the individual has agreed, by e-mail. This notification must be done within a maximum of 60 days after the discovery of the breach.

If the practice has insufficient contact information for fewer than 10 individuals affected by the information, alternative contact, such as a telephone call or written notification to an alternate address provided by the individual, may be used. If the practice has insufficient contact information for 10 or more affected individuals, it must:

- Post the notification on its web site, or
- Provide notification in major print or broadcast media where the affected individuals likely reside.

The notification, regardless of mechanism, must include the following information:

- A description of the breach
- A description of the types of information involved in the breach
- Steps the affected individuals should take to protect themselves from potential harm
- What the practice is doing to investigate the breach, mitigate the harm, and prevent further breaches
- Contact information for the practice

(Continued on next page)

## SPECIAL FEATURE

Notices posted via print or broadcast media or online must include a toll-free number individuals can use to contact the practice to determine if their information was included in the breach.

### MEDIA NOTICE

If more than 500 individuals were affected by the breach, the covered entity must also provide notification to prominent media outlets serving the area where the patients reside. This should be in the form of a press release provided within 60 days of the breach discovery, and must include the same information used in the individual notice.

### NOTICE TO THE SECRETARY

In addition, this practice must notify the HHS Secretary. This must be done electronically through the HHS web site, using the form entitled "Notice to the Secretary of HHS of Breach of Unsecured Protected Information." The form is available online at <http://transparency.cit.nih.gov/breach/index.cfm>.

For a breach affecting more than 500 individuals, this notification must be done within 60 days. If the breach affects fewer than 500, the report(s) may be done annually, no later than 60 days after the end of the calendar year in which the breach(es) occurred. +

*Ms. Bachman is director of the Compliance Department at DoctorsManagement; contact her at [abachman@drsmgmt.com](mailto:abachman@drsmgmt.com) or 800-635-4040.*

*DoctorsManagement, LLC, is a TMA Corporate Partner. This information was supplied by DoctorsManagement exclusively and for the benefit of our members. The TMA does not accept responsibility for the information provided.*



*St. Jude patient*

**Honor a friend . . .  
Remember a loved one.**

Honor the accomplishments of a friend or remember a loved one by making a donation in their name to St. Jude Children's Research Hospital, the premier pediatric cancer research center.

**Give the gift of life to children around the world.**

St. Jude Children's Research Hospital  
Memorials and Honors  
P.O. Box 1000, Dept. 142  
Memphis, TN 38148-0142  
1-800-873-6983  
[www.stjude.org/tribute](http://www.stjude.org/tribute)

**St. Jude Children's  
Research Hospital**  
ALLIANCE • DEDICATED • TOGETHER

*Finding cures. Saving children.*

# MOVING? Send Us Your New Address!

*Please notify us six weeks in advance.*

Old Address \_\_\_\_\_ City \_\_\_\_\_ St \_\_\_\_\_ Zip \_\_\_\_\_

Name \_\_\_\_\_ Practice Name \_\_\_\_\_

New Address \_\_\_\_\_ City \_\_\_\_\_ St \_\_\_\_\_ Zip \_\_\_\_\_

Fax \_\_\_\_\_ Phone \_\_\_\_\_ E-Mail \_\_\_\_\_

Effective Date of New Address \_\_\_\_\_

*Send to: TMA Membership Department, PO Box 120909, Nashville, TN 37212-0909*