



*WHAT YOU NEED TO KNOW ABOUT THE
NEW HIPAA REGULATION RELATING
TO DATA BREACH NOTIFICATION*

*45 CFR Parts 160 and 164 Breach Notification for
Unsecured Protected Health Information*

Daniel F. Bayha, Vice President

Back Thru The Future Technology Disposal
150 Main Street
Ogdensburg, NJ 07439
973-823-9752
shred@backthruthefuture.com

DATE: October 1, 2009

45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information

On September 23, 2009, the Department of Health and Human Services enacted a new rule as part of the HITECH provision of the American Recovery and Revitalization Act (ARRA). The data breach notification is meant to significantly augment HIPAA privacy requirements.

Data breach notification has been a part of most State ID theft regulations for many years. The single biggest impact this regulation has had on the financial industry is that it makes data breaches public along with the resulting public relations problems. A Wall Street Journal study found that a publicly traded company that acknowledges a data breach can expect its stock to drop between 2-3% within the following three weeks.

There are also real costs associated to the notification process which includes the notification itself and three months of toll free telephone access for affected individuals. The cost per affected individual has been estimated by ID theft organizations at \$50-60.

Organizations need to be fully compliant with these regulations to avoid penalties and reputational loss.

What is considered a “Data Breach”?

The statute defines a “breach” as the “unauthorized” acquisition, access, use, or disclosure of protected health information (PHI).

Who is a “Covered Entity” under the regulation?

These breach notification provisions are found in section 13402 of the Act and apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information

How does this provision affect my “Business Associate’s” agreements?

Any business activity defined under “covered entity” performed by a vendor requires a business associate’s agreement with the requirement to notify the covered entity in the event of a data breach.

Who must be notified in the event of a data breach?

- **Less than 500 affected individuals:** The covered entity must maintain a log documenting the breaches and annually report the activity to the Secretary of HHS.
- **More than 500 affected individuals:** The covered entity must immediately, in no case longer than 60 days after the discovery of a breach, notify the Secretary of HHS and the affected individuals. In addition, the covered entity must provide notice to “prominent media outlets” in the state or jurisdiction where the breach occurred.

Business Associate Breach: The Business Associate must notify the covered entity within 60 days of the discovery of a breach. The Business Associate must notify the Secretary of HHS of the breach but the covered entity is responsible for the notification to individuals affected.

What is “Unsecured Protected Health Information”?

Section 13402(h) of the Act defines “unsecured protected health information” as “protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance”

What is the Secretary’s “guidance” for the technology or methodology to secure protected health information?

Encryption:

- i. Valid encryption processes for data at rest are consistent with NIST Special Publication 800–111, *Guide to Storage Encryption Technologies for End User Devices*.^{3 4}
- ii. Valid encryption processes for data in motion are those which comply, as appropriate, with 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*

Destruction of the Media

- i. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
- ii. 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.

What is the “Secured Data” exclusion?

Covered entities and business associates that implement the specified technologies and methodologies with respect to protected health information are not required to provide notifications in the event of a breach of such information—that is, the information is not considered “unsecured” in such cases.

Standards for electronic media destruction vary, however, the most assured and cost effective process for compliant eradication is by shredding, disintegrating, or pulverizing.

*NIST Special publication 800-88
Guidelines for Media Sanitization*

Clear = Good Purge = Better Destroy = Best

Hard Drives:

Clear: Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.

Purge: Purge hard disk drives by either purging the hard disk drive in an NSA/CSS approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand

Destroy: Shred, Disintegrate, Pulverize, Incinerate

Tape:

Clear: Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods

Purge by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be accomplished easier by using an NSA/CSS-approved degausser for the magnetic tape

Destroy: Shred, Disintegrate, Pulverize, Incinerate

Back Thru the Future can help organizations achieve full compliance and proactively ensure that any electronic media destruction is handled in accordance with guidelines for "secured data".

Healthcare organizations routinely contract for paper shredding service but do not typically give the same amount of destruction diligence to electronic media. The loss of a single sheet of paper might compromise a single patient's protected health information. A lost hard drive can compromise thousands of patient records. Reduce your liabilities associated to data breach notification. Secure your electronic data by destroying the media.

As one of only a handful of NJ DEP licensed electronic recycling facilities with a shredding operation, we guarantee complete irreversible destruction for media. Our Safe Harbor Express service was designed with compliant processing in mind. Safe Harbor provides a "routinized" pick up schedule, securitized containers, and point-to-point transport for a single annual fee.

To learn more about Safe Harbor Express,
contact Back Thru The Future at shred@backthruthefuture.com.