Mandatory Data Breach Notification

On February 18, 2009, the United States Congress passed the Health Information Technology for Clinical and Economic Health (HITECH) Act, which dramatically increased the enforcement of HIPAA's data security provisions.

The new security provisions included

- **Mandatory Health Data Breach Notification**
- Increased Penalty Limits *(going from $25,000 to $1,500,000)*
- States' Attorneys General Enforcement
- Revision of All Business Associate Agreements
- Mandatory Fines for HIPAA Violations

Here is how the US Department of Health and Human Service (HHS), the agency responsible for overseeing HIPAA enforcement, outlines the new mandatory health data breach notification.

Breach Notification Requirements
Following a breach of unsecured protected health information covered entities must provide **notification** of the breach to **affected individuals, the Secretary (HHS), and, in certain circumstances, to the media**.

Definition of Breach
A breach is, generally, an impermissible use or **disclosure** under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

Unsecured Protected Health Information and Guidance
Covered entities and business associates must only provide the required notification if the breach involved unsecured protected health information. **Unsecured** protected health information is any information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance.

Paper, film, or other hard copy media must be 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.

Electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

MORAL: Any casually discarded patient information, whether on paper media or electronic media, requires that the healthcare provider conduct the required Data Breach Notification.

Extremely large fines have already been assessed to health care providers who have failed to conduct the required Data Breach Notification after such an event. Read more about these and other consequences of improper PHI disposal in Recent News.

Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html