Breach response and HIPAA
Understanding the final omnibus rule

The omnibus rule expands the definition of what constitutes a breach and requires a documented risk assessment to determine breach status and notification requirements.

• Then: The 2009 Interim Final Rule asked organizations to assess the risk of harm to affected individuals in determining whether the incident qualified as a breach.

• Now: The omnibus rule establishes much broader guidelines. Organizations must now assess the probability of compromise for the data that was lost.

The “harm standard,” as the Interim Final Rule’s assessment guideline was known, was simply too subjective. A recent study confirms that, if a breach were to occur, only 23 percent of organizations could pinpoint the actual or potential harm facing victims.¹

¹ Data Breach Readiness Study, Ponemon Institute (2013)

Legal Notice
The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

© 2013 Experian Information Solutions, Inc. All rights reserved. Experian and the marks used herein are service marks or registered trademarks of Experian Information Solutions, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners.
BUSINESS ASSOCIATES

More types of businesses, such as data transmission services and patient safety organizations, are now considered business associates and thus liable under the Security Rule and various provisions of the Privacy Rule.

• Then: Business associate agreements (BAAs) between covered entities and business associates were mandatory.

• Now: BAAs are also now required between business associates and their subcontractors that handle, process or otherwise access PHI.

Business associates, not covered entities, are responsible for ensuring their subcontractors comply with the Privacy and Security Rules. Be sure your BAAs specifically outline your data handling policies.

BREACH NOTIFICATION

The omnibus rule notes that covered entities are ultimately responsible for breach notification, though they may delegate the task to the business associate that caused the breach. The omnibus rule also clarifies several notification issues:

• A press release on a covered entity’s website does not fulfill the media notification requirement; a press release to media outlets located where affected individuals reside does

• Reporting a breach involving 500 or more individuals “immediately” to HHS means at the same time an organization notifies those affected

• In lieu of a risk assessment, covered entities and business associates can notify all affected individuals

ACCELERATED BREACH RESPONSE

The complexities of the HIPAA Omnibus Rule will forever change your breach response, so be sure your data breach resolution provider is up to the task of helping you comply with the new regulations.

Experian® Data Breach Resolution is a trusted business associate for thousands of healthcare companies. In 2012, 40 percent of the breaches we serviced were in healthcare.

EXPERIAN DATA BREACH RESOLUTION HELPS YOU TO:

• Accelerate your understanding of the HIPAA Omnibus Rule

• Be ready when a breach strikes with cost-saving, pre-breach agreements

• Institute data breach services in accordance with HIPAA guidelines

• Reduce the likelihood of devastating penalties and fines

We’re always ready to act with proven solutions that have been field-tested by Fortune 500 companies, government agencies and companies in nearly every industry. We’re the experienced breach response team you can call on in a crisis.

BE MORE THAN READY. BE HIPAA READY WITH EXPERIAN.

For more information, call 866-751-1323 or email databreachinfo@experian.com

Visit us online: Experian.com/DataBreach
Follow us on Twitter: @Experian_DBR
Read our blog: Experian.com/DBBlog
Download our free mobile app for iPhone or Android

FOUR QUESTIONS TO ASK DURING A RISK ASSESSMENT

1. What’s the nature and extent of PHI involved (include types of identifiers and the likelihood of re-identification)?

2. Who is the unauthorized person or party who used the PHI or to whom was the disclosure made?

3. Was PHI actually acquired or viewed?

4. To what extent has the risk to the PHI been mitigated?