

# HIPAA BREACH NOTIFICATION RULE – THE TIME TO COMPLY IS NOW!

By Jeanine Freeman

Medical ethics recognize the risk of breaches of patient information. “[D]etailed and complex patterns of collecting and using patient information in today’s health care environment mean that the risk of harm to patients from security breaches is higher than ever before,” cautions the AMA’s Council on Ethical and Judicial Affairs (CEJA) in its report, “A Physician’s Role Following a Breach of Electronic Health Information.” Information breaches can harm the patient and impair the physician-patient relationship. “Helping to restore a sense of control over health records to the patient is of great moral import.” Health information breaches should be voluntarily and promptly disclosed.

HIPAA rules now specify notification processes that physician covered entities and their business associates (BAs) must follow upon discovery of a reportable breach of protected health information (PHI) whether in electronic, paper or oral form. Adopted within the context of the HITECH (Health Information Technology for Economic and Clinical Health) Act, the breach notification rule became effective on September 23, 2009. However, the federal Department of Health and Human Services (HHS) will exercise enforcement discretion and will not impose sanctions until February 22, 2010, as practices come into compliance by, for instance, amending their notices of privacy practices and BA agreements consistent with the rule.

By definition, a “breach” is an impermissible acquisition, access, use or disclosure of “unsecured” PHI that compromises the security or privacy of that PHI. If a data breach does not involve PHI as defined by the HIPAA Privacy Rule, the notification rule does not apply. If the breach involves secured PHI, notification is

not required. PHI is “secured” if it is unusable, unreadable, or indecipherable to unauthorized individuals through technologies (i.e., encryption) or methodologies (i.e., destruction) recognized by HHS consistent with guidance set out in the rule’s comments.

A breach of unsecured PHI requires notification only if the breach “compromises the security or privacy” of the PHI by posing “a significant risk of financial, reputational, or other harm to the individual.” A risk assessment is required; the rule and its comments provide helpful guidance on what to look for in and how to document such an assessment. A breach involving a limited data set (as defined by the HIPAA Privacy Rule) absent zip codes and dates of birth is exempt from notification. Other exceptions, such as an impermissible disclosure unintentionally made in good faith in the course of business and not further disclosed, are set forth in the rule and its comments.

Notification of reportable breaches must take place “without unreasonable delay” and in no case later than 60 calendar days after “discovery” – the first day on which the breach is known or, with reasonable diligence, would have been known. Notification shall be written in plain language. HHS must be notified in writing at the same time if the breach involves more than 500 individuals; if less, the breach must be logged and HHS notified within 60 days of the end of the calendar year. The media must be notified for breaches involving more than 500 residents of a state or jurisdiction.

Access the rule and its comments (your best guide) at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breach-notification-rule.pdf>. AMA guidance is available at <http://www.ama-assn.org/ama1/pub/upload/mm/399/hipaa-breach-notification-rule.pdf>.



Jeanine Freeman, JD, is Senior Vice President of Legal Affairs for the Iowa Medical Society.