HIPAA Policy No. 9

Breach Notification

Conducting an Investigation and Risk Assessment

All patient complaints or other discoveries of potential breaches of privacy policies shall be reported immediately to the practice's Privacy Officer. The Privacy Officer, with the assistance of counsel if necessary, will conduct and document a risk assessment to determine whether the use or disclosure constitutes a "Breach" as that term is defined by the HIPAA Breach Notification Rule, noting that an unauthorized use or disclosure will be presumed to be a breach unless the risk assessment demonstrates that there is a low probability that the protected health information has been compromised. The risk assessment must be based on at least the following factors:

(1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(2) The unauthorized person who used the protected health information or to whom the disclosure was made;
(3) Whether the protected health information was actually acquired or viewed; and
(4) The extent to which the risk to the protected health information has been mitigated

Breach Notification Procedures: Individual Notice

If the practice, after conducting the Breach Notification risk assessment, reasonably believes that an unauthorized use or disclosure meets the definition of a Breach, as discussed above, the Privacy Officer or a designee shall conduct the following breach notification procedures:

- Written notice to all individuals whose protected health information was involved in the incident at the individuals' last known address by first-class mail (or by electronic mail if specified by the individual). Written notice may be made to the individual's next of kin (if the individual is deceased) or personal representative (if the individual is a minor or incapacitated).
- Substitute notice to all individuals for whom the practice has insufficient or out-of-date contact information. In cases involving fewer than 10 such individuals, substitute notice can be by an alternative form of written notice, by telephone notice or by any other means. In cases involving 10 or more such individuals, substitute notice may be made either by a conspicuous posting on the home page of the practice's website or by publication in a major print or broadcast media.
- Notification by telephone or other method may be made *in addition to the above notices* in cases in which the Privacy Officer deems urgent based on the possibility of imminent misuse of the individual's protected health information.

Contents of Notice

An individual notice of breach must include the following information, to the extent the information is available:

- A brief description of the incident, including the date of the breach and the date of discovery of the breach;
- A description of the types of unsecured information that were involved in the breach;
- Any steps that the affected individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the practice is doing to investigate the incident, mitigate harm to the affected individuals, and protect against further breaches; and
- Contact procedures for affected individuals to ask questions or learn additional information, including either a toll-free telephone number, e-mail address, website or postal address.

Timing of Notice

The Privacy Officer shall notify affected individuals without unreasonable delay, but in no case later than 60 days after discovering the incident.

Breaches Involving More Than 500 Individuals

If the incident involves more than 500 affected individuals, the Privacy Officer must be notified immediately. The Privacy Officer will determine whether and when notice to the individuals, the media, and/or the Secretary of HHS is appropriate.

Tracking Breaches

The Privacy Officer will maintain a log of all breaches and notifications. The Privacy Officer will submit combined reports annually to the Secretary of HHS, as required through the OCR's website at:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Authorities:

HITECH Act, Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009 (effective Feb. 17, 2009)
HITECH Act Breach Notification Interim Final Rule (effective Sept. 2009)
Omnibus Final Rule

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, Final Rule, 78 *Fed. Reg.* 5566 (January 25, 2013)