

## BE CAREFUL: Steps Practices Should Take to Avoid Significant Penalties When There is a Breach of Patient Records

*Michael F. Schaff, Esq. and Glenn P. Prives, Esq. - Wilentz, Goldman & Spitzer, P.A., Woodbridge, New Jersey*

The failure of a practice to notify patients of the breach of their Protected Health Information (PHI) may result in the practice being sanctioned by the Department of Health and Human Services (HHS). Most administrators are aware that PHI is health information that can be attributed to an individual. When the practice discovers a breach of PHI, the practice must notify all affected patients in order to comply with the Health Information Technology for Economic and Clinical Health Act (HITECH).

What is a breach? A breach is deemed to have occurred when PHI is accessed or disclosed without authorization. However, if it is a one-time access or inadvertent disclosure by an authorized person that was made in "good faith," it is not a breach. Importantly, if the PHI is encrypted (unreadable, unusable or indecipherable), there is no notification to patients required.

Upon a PHI breach, notification to patients must be made no later than 60 days following the breach, with few exceptions. Practices must notify all affected patients by first class mail and send notice to the last known address of the patient or to the next of kin if the patient is deceased. However, if the patient, prior to the breach, chose to be notified of a breach by email, the practice need only provide the required notification by email. Therefore, it is advisable to have patients consent, in writing, upon a visit, to notification by email. A simple form can be provided to the patient to obtain consent, which should include a place for the patient to provide his or her email address. Where the patient's contact information is out-of-date and fewer than 10 patients are affected by the breach, a practice may notify patients by phone, email, or if there is no contact information, a posting on the practice's website.

If the breach affects 10 or more patients, a practice may make a posting on its website, if it has one, for 90 days or a media announcement in the areas where the affected patients reside. Consequently, it is prudent to establish at least a rudimentary website in the event that a breach does occur to avoid having to notify each patient individually. If the affected patient is a minor or lacks legal capacity, notice to the guardian or the personal representative of the patient is sufficient.

If more than 500 patients are affected by a breach of PHI, in addition to individual notice, the practice must provide notice through a newspaper, radio or television. HITECH also requires the practice to notify the Secretary of HHS of the breach. If the breach affects fewer than 500 patients, the practice may submit notice of all breaches together in an annual log to the Secretary of HHS, no later than 60 days after the conclusion of the calendar year. For breaches affecting 500 or more patients, the notice must be provided to the Secretary of HHS at the same time it is provided to the patients. The Secretary of HHS will post the name of the practice on its website.

What should be in the notification? The notification to patients must include the following information:

- A description of what happened, including the date of the breach and the date of discovery;
- A description of the PHI that was involved in the breach;
- Steps the patients should take to protect themselves;
- A description of what the practice is doing to investigate, to lessen the harm to the patients, and to protect against further breaches; and
- Contact information for questions.

Practices must establish policies and procedures to be followed when discovering a breach, including a complaint system by which affected patients may register complaints regarding these procedures. They must make employees aware of these procedures and must have sanctions in the event employees do not follow these policies.

Practices will be sanctioned for failing to comply with these requirements:

NATURE OF VIOLATION	RANGE OF PENALTIES	MAXIMUM PENALTY
Violation unknown or would not have known	\$100 for each violation, up to \$25,000 for all violations in a calendar year	\$1.5 million for all violations
Violation due to reasonable cause	\$1,000 for each violation, up to \$100,000 for all violations in a calendar year	\$1.5 million for all violations
Violation due to neglect, if corrected within thirty (30) days from knowledge of violation	\$10,000 for each violation, up to \$250,000 for all violations in a calendar year	\$1.5 million for all violations
Violation due to neglect not corrected	\$50,000 for each violation, up to \$1.5 million for all violations during a calendar year	\$1.5 million for all violations

So be careful. Each practice should take the above steps when it has discovered a PHI breach. HITECH requires the practice to demonstrate compliance and failure to do so may result in steep penalties for a practice.