

LAW OFFICES

**ROLAND & SCHLEGEL**

A LIMITED LIABILITY COMPANY  
627 NORTH FOURTH STREET  
P.O. BOX 902  
READING, PA 19603-0902  
(610) 372-5588  
FAX (610) 372-5957  
firm@rolandschlegel.com  
www.rolandschlegel.com

OLEY OFFICE  
308 MAIN STREET  
OLEY, PA 19547  
(610) 987-3277

FLEETWOOD OFFICE  
12 WEST MAIN STREET  
FLEETWOOD, PA 19522  
(610)-944-6870

JOHN W. ROLAND  
EDWIN L. STOCK  
S. WHITNEY RAHMAN  
ROBERT R. KREITZ  
JOHN E. MUIR  
DEBORAH A. SOTTOSANTI  
DANTE C. CUTRONA  
GREGORY A. SHANTZ

OF COUNSEL TO THE FIRM  
DAVID H. ROLAND  
MARY M. BERTOLET  
JERRY R. RICHWINE

RAYMOND C. SCHLEGEL (2004)  
D. FREDERICK MUTH (2006)

**\*\*EMPLOYMENT LAW ALERT\*\***

**How the HITECH Act May Affect You**

By: S. Whitney Rahman

As part of the recovery plan of 2009, Congress passed the Health Information Technology for Economics and Clinical Health (HITECH) Act. This Act amends HIPAA, the Health Improvement Portability and Accountability Act, in key ways, some of which are discussed below.

First, it extends security provisions and penalties to the business associates of covered entities. HITECH Act, Section 13404. Previously, the law contained no provisions for penalties against business associates. Now, business associates will be held to the same standards as covered entities for purposes of the imposition of penalties. Accordingly, business associates need to be more vigilant than ever in ensuring the security of protected health information on behalf of the covered entity.

Second, the Act creates a new responsibility for both covered entities and business associates to provide notice of breaches of security. It requires that covered entities provide notification of breach to individuals whose personal health information (PHI) was acquired by an unauthorized person as a result of a breach of security. They also must notify the Federal Trade Commission of the breach.

Third party service providers that discover a breach of security are required to notify the entity for which it provided service. The notice must identify each individual whose identifiable health information has been or is reasonably believe to have been, accessed, acquired, or disclosed during the breach. HITECH Act, Section 13407(b).

A breach of security is defined as the acquisition of identifiable personal health information without authorization of the individual to whom the information pertains. HITECH Act, Section 13407(f)(1).

HITECH Act, Section 13407(g). The regulations further define the responsibilities of covered entities and business associates under the Act.

The interim regulations specify that a breach is considered to be “discovered” as of the first day the breach is known to the entity, or should have been known through reasonable diligence. 45 C.F.R. § 164.404(2). Unless notification of the breach would impede a criminal investigation, and the entity has been so informed by a law enforcement official, notification must be made without unreasonable delay, and in no case later than 60 calendar days after the discovery of a breach. 45 C.F.R. § 164.404(b).

Under the interim regulations, the notice must be written in plain English, and must include, to the extent possible:

- (1) A brief description of what occurred, including the date of the breach and the date of its discovery;
- (2) A description of the types of unsecured PHI involved (whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- (3) Steps that individuals should take to protect themselves from potential harm resulting from the breach;
- (4) A brief description of what the covered entity is doing to investigate the breach, mitigate harm and protect against future breaches; and,
- (5) Information about who to contact if individuals have questions or want more information. The contact information must include a toll-free telephone number, e-mail address, website or mail address.

45 C.F.R. § 164.404(c).

Notice must go to the individual by first-class mail at the last known address, or by e-mail, if the individual has agreed to e-mail notification. If the entity knows the individual is deceased, notice should be sent to the next of kin or the individual’s personal representative. 45 C.F.R. § 164.404(d)(1). If the covered entity deems the situation urgent, it may also provide information by telephone or other means. 45 C.F.R. § 164.404(d)(3).

If there is insufficient contact information, the entity must use a substitute form of notice that is reasonably calculated to reach the individual. If there is insufficient contact information for more than ten individuals, substitute notice must either consist of a conspicuous posting on the entity’s website for a period of 90 days, or a conspicuous notice in a major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside. In either case, the notice must contain a toll-free telephone number that is active for at least 90 days to inform individuals whether their information has been compromised. 45 C.F.R. § 164.404(d)(2).

In addition to notice to the individual and the Federal Trade Commission, the regulations require that, if the breach involves more than 500 residents of a state or jurisdiction, the entity must notify prominent media outlets serving that state or jurisdiction. 45 C.F.R. § 164.406(a).

The entity also must notify the Secretary of Health and Human Services (“HHS”) following discovery of a breach. If the breach involved 500 or more individuals, notice to the Secretary of HHS must be provided simultaneously with notice to the individuals and media. If the breach involves fewer than 500 individuals, the covered entity must maintain a log or other documentation of the breach and, within 60 calendar days after the end of each calendar year, provide notification to the Secretary of all breaches during the previous calendar year. 45 C.F.R. § 164.408. The HHS website contains information as to how this report must be made.

Note that the regulations are not consistent in this regard. Thus, while 45 C.F.R. § 164.406(a) requires notice to prominent media outlets if more than 500 residents are affected, notice to the Secretary is required if the breach involves 500 or more individuals, not if it involves more than 500 individuals. 45 C.F.R. § 164.408.

If a business associate of a covered entity discovers or reasonably should have discovered a breach, it must notify the covered entity, within 60 days of that date of discovery or when it reasonably should have been discovered. 45 C.F.R. § 164.410. The business associate notification should include the same information to the covered entity as the covered entity is required to provide to the individual. 45 C.F.R. § 164.410(c).

The covered entity or business associate has the burden of proving that it made notification as required under the regulations, or alternatively, showing that the use or disclosure was not a breach. 45 C.F.R. § 164.414(b). It must maintain documents sufficient to make this showing. 45 C.F.R. § 164.530 (i)(1)(iv).

In addition to the notice requirements, covered entities must train all employees on policies and procedures related to protected health information and related to the required notices. 45 C.F.R. § 164.530. Covered entities also must have in place and enforce sanctions against employees who do not comply with the privacy procedures of the covered entity or do not comply with federal regulations. 45 C.F.R. § 164.530(e)(1).

Covered entities also must provide a process for individuals to lodge complaints about the covered entities’ procedures related to protected health information and required notices. 45 C.F.R. § 164.530(d)(1).

Covered entities may not retaliate, discriminate, intimidate, threaten or coerce an individual for exercise of any rights under HIPAA’s privacy provisions. 45 C.F.R. § 164.530(g)(1). Covered entities also may not require individuals to waive their rights under the privacy provisions of HIPAA as a condition of participation in the covered entity’s programs. 45 C.F.R. § 164.530(h).

The notice provisions of the HITECH Act became effective on September 23, 2009, 30 days after the promulgation of the interim regulations. The portions of the act expanding

enforcement to business associates becomes effective as of February 17, 2010, one year after enactment of the Act.

### What This Means To You

If your workplace is a covered entity under HIPAA, if it administers a health care plan, or if it provides services to covered entities as a business associate, the HITECH Act provides new responsibilities that you need to be aware of. Companies will need to develop policies and training modules in compliance with the regulations.

The notice requirements are rigorous and the best case scenario is never to need to invoke them. Accordingly, it is more important than ever that companies ensure that they safeguard personal health information.

If you need further information about HITECH Act, please contact S. Whitney Rahman or John Roland at 610-372-5588.