



To notify, or not to notify?

Depends on privacy insurance policy forms and state notification

Insurance coverage highlights from South Shore Hospital breach

In July 2010, the South Shore Hospital in Weymouth, MA announced that computer files containing personally identifiable information had been lost. The lost files were stored on back-up computer tapes that had been sent to a service provider for destruction. The tapes never reached their destination. The South Shore Hospital disclosed the loss of the data on its website and notified federal and state authorities. Its website explanation was accompanied by a sample notification letter that the Hospital anticipated sending to the affected individuals. The sample letter had a toll-free number for affected people to call and learn how to protect themselves from identity theft, and it offered them a free credit report.

The South Shore Hospital engaged forensic specialists to investigate the the breach and assess the likelihood that confidential personal information was actually compromised. The specialists determined that the information was probably sent in sealed boxes to a commercial landfill. The information was not encrypted, but the Hospital said the information could not be read without specialized equipment and software. The Hospital indicated that there was "little to no risk" that third parties could gain access to the information.

The Hospital concluded that it was not legally required to send notices to each of the affected individuals by posted mail. Instead, the Hospital said that it will provide "substitute" notice in Massachusetts' largest newspapers and through postings in the affected organizations and doctors' offices. The Hospital said it would provide notice by email when it obtains the relevant email addresses. Such substitute notice is permitted under Massachusetts law "if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed \$250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice."

Massachusetts Attorney General Martha Coakley has objected to the Hospital's decision to forego individual notices. At least one commentator has questioned whether the Hospital is excused from notifying all the affected individuals. The August 2009 interim notice rule promulgated under HIPAA excuses notification of affected individuals if the compromised data is encrypted or otherwise unreadable or indecipherable. This federal rule preempts "contrary" state law, although it is not clear whether the Hospital is claiming exemption from individual notification (i) based on the seemingly contrary Massachusetts provision for substitute notice described above, or (ii) based on the federal exemption applicable to data that cannot be read. When its forensic investigation was completed, the Hospital concluded, but apparently did not prove, that the data was likely deposited in a commercial landfill and is inaccessible to third parties.

This is not an idle matter. If the Hospital were to provide individual notice, its provenance could determine whether or not it would be covered by insurance. **The trigger for insurance coverage is not the same under every privacy policy.** For starters, many policies labeled as "privacy" insurance don't provide any coverage for the costs incurred in providing notice to affected individuals. Even for those that do, the trigger for commencing coverage may depend on why notice is provided, although this can often be negotiated. An organization should not simply assume that the costs of providing notice to individuals will automatically be covered by its privacy insurance policy – even though most would surely consider this to be one of the core coverages under that type of policy.

The South Shore Hospital notice conundrum highlights another aspect of privacy insurance coverage: **who pays the costs incurred in determining who has to do what?** Many different expenses fit within the category of “figuring things out.” These can include the legal costs incurred in determining whether notice to individuals is required under applicable law, the legal costs incurred in notifying all applicable governmental agencies of the breach, and the potentially mammoth forensic investigation costs that can be incurred in determining the source and extent of the breach.

As is the case with most aspects of coverage in this rapidly developing area of insurance, different policy forms yield different answers -- and many initially unfavorable policy provisions can be negotiated for the benefit of the insured. Companies should not be lulled into complacency about the scope of their insurance protection simply because they have a policy or endorsement with the words “privacy” or “security” in its title. They need to give focused thought to their needs and make sure that their insurance policy’s language reflects their coverage expectations.

For more information regarding privacy insurance policies, contact your WGA Client Executive or visit www.privacy-insurance.com.



John Doernberg, Vice President, *William Gallagher Associates* 617.646.0336 joernberg@wgains.com

After practicing law at top law firms for twelve years, since 1995 Mr. Doernberg has been an insurance broker focusing on complex coverages. He received his undergraduate degree, cum laude, from Yale College in 1979 and his law degree from Columbia Law School in 1982. Drawing on his legal background, Mr. Doernberg serves as a bridge among clients, their lawyers and underwriters in structuring insurance programs and negotiating and drafting endorsements to address complex coverage matters. At WGA he is responsible for developing relationships and serving as a resource for WGA clients when complex coverage issues require customized solutions, with a particular focus on privacy and data security issues.