Insights, News & Events

HHS ISSUES HIPAA SECURITY-BREACH-NOTIFICATION RULES: COMPLIANCE DEADLINE LOOMING

Insights
Sep 1, 2009

On August 24, 2009, the Department of Health and Human Services (HHS) issued interim final rules regarding the new security-breach-notification requirement of the Health Insurance Portability and Accountability Act (HIPAA). Covered entities and their business associates (service providers to covered entities) only have 30 days after publication (or until September 23, 2009) to comply with these new rules.

Background
Among other changes, a new rule requires covered entities (including group health plans and healthcare providers) to notify individuals when their "unsecured" protected health information (PHI) is breached. There is a significant exception to the breach-notification requirement for breaches of "secured PHI." Secured PHI is PHI maintained in accordance with the most current HHS guidance specifying the safe-harbor technologies and methodologies that render PHI unusable, unreadable or indecipherable by unauthorized persons.

Last April, HHS issued its first guidance as to what an entity must do to secure PHI, including a specific level of encryption and specific types of destruction. HHS expects to update this guidance annually. Covered entities and business associates which satisfy the current HHS safe-harbor technologies and methodologies are not required to send notices to individuals upon a breach of PHI.

If required, the notification of breach must be provided to individuals within 60 days after discovery of the breach (or the day the entity should have discovered the breach if it had been prudent in its HIPAA compliance efforts). The notice must be provided by first-class mail unless email was previously approved by the individual for delivery of such notice. If the breach involves 500 or more individuals' PHI, the covered entity must also notify the media and HHS immediately. If fewer than 500

individuals are affected, the covered entity must log the breach and submit it annually to HHS.

Business associates must notify covered entities of their breaches so that covered entities can timely meet the notice requirements. But, a business associate and a covered entity can agree, as part of the business-associate agreement, that the business associate will notify affected individuals directly in case of a breach by the business associate.

What Is A Breach?
The new rules provide that there is a "breach" where there is an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rules, and such action compromises the security or privacy of the PHI. PHI is compromised only if the event poses a significant risk of financial, reputational, or other harm to the individual.

The definition of a breach specifically *excludes* the following scenarios:

- unintentional access by a covered entity's employee or business associate acting under authority;
- inadvertent disclosure from one covered entity or business associate employee authorized to access PHI to a co-employee authorized to access PHI; and
- unauthorized access by an unauthorized person who cannot reasonably be able to retain the information disclosed.

Notification To Individuals
In the event of a breach, the covered entity must notify the individual "without unreasonable delay," but no later than 60 days after the discovery of the breach. The notice must be written in plain language and contain:

- a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- a description of the types of PHI involved in the breach (such as full name, social security number, date of birth, home address, account number, diagnosis, disability code, etc.);
- suggested steps individuals should take to protect themselves from potential harm resulting from the breach;
- a brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

- contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, website, and postal address.

What Plans And Their Business Associates Should Do Now

Covered entities and business associates will need to act quickly in order to comply with the new rules by September 23, 2009. First, covered entities and business associates need to determine if they satisfy the HHS safe harbor and if so, update their HIPAA Privacy policies and procedures to reflect this. Any entity that does not satisfy the safe harbor needs to develop internal procedures to determine when a breach has occurred as well as the method and responsibility for risk assessment, distributing individual notifications, notifying the media and HHS and mitigation. These entities must update their HIPAA Privacy policies and procedures to reflect this new internal policy.

Fisher Phillips has developed two new HIPAA Privacy Policies (one for those entities which satisfy HHS' safe harbor and one for those who do not) to update our HIPAA Privacy Compliance Package, which allows group health plans and business associates to comply with the new rules before the September 23, 2009 compliance deadline.

Covered entities and business associates may purchase the relevant additional HIPAA Privacy Policy, customized for the plan's or business associate's ability to meet the current HHS safe harbor for secured protected health information. For group health plans which have not yet completed their HIPAA Privacy and Security compliance, we recommend they complete these reviews as soon as possible, as the new law also mandates that HHS begin random auditing of covered entities' HIPAA compliance.

This Legal Alert presents an overview of the requirements of a specific federal rule. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.