HIPAA Breach Notice Rules

New notice requirements for HIPAA covered entities when there is a breach of Protected Health Information (PHI)

On August 24, 2009, the Department of Health and Human Services ("HHS") issued regulations implementing new HIPAA breach notice rules. The rules require HIPAA covered entities, including employer-sponsored health plans, to notify affected individuals and HHS (and sometimes prominent media outlets) upon discovery of a breach of an individual's unsecured protected health information ("PHI"). **Failure to provide notice, or to properly document how breaches are handled, can result in significant penalties.** Although the new rules are effective for breaches discovered on or after September 23, 2009, the regulations indicate that HHS will not impose sanctions for failure to provide breach notices until February 22, 2010. The following summarizes the new rules.

What are the HIPAA breach notice rules? The breach notice rules were enacted by section 13402 of the American Recovery and Reinvestment Act of 2009 ("ARRA"). The rules establish new notice requirements for HIPAA covered entities. The notice requirements apply if a covered entity (or its business associate) discovers a breach of an individual's PHI. Unless an exception applies or the covered entity concludes that the breach does not pose a significant risk of harm, a covered entity must notify the affected individual and HHS. If a breach affects more than 500 residents of the same State, the covered entity is also required to notify prominent media outlets. The breach notice rules do not preempt State breach notice laws unless the State law is "contrary" to the federal law (and a State law is contrary only if a covered entity would find it impossible to comply with both the State law and the federal law).

Do the breach notice rules apply to secured PHI? No. The breach notice rules apply only to unsecured PHI-they do not apply to secured PHI. However, PHI is treated as "secured" only if it satisfies one of the following requirements: (1) electronic PHI is secured only if it complies with specific encryption standards issued by the National Institute of Standards and Technology ("NIST")[1] or is destroyed in accordance with NIST media sanitization standards[2]; and (2) paper PHI is secured only if it is shredded or destroyed so that it can't be read or reconstructed. Most employer-sponsored health plans do not encrypt all forms of electronic PHI, nor do they typically destroy all forms of electronic or paper PHI.

What is a breach? A "breach" is defined broadly as a use or disclosure of an

individual's unsecured PHI that violates the HIPAA privacy rule and creates a significant risk of financial, reputational or other harm to the individual. Following a possible breach incident, the new rules require covered entities to review the incident and determine whether a breach occurred. This review should include three elements: (1) a determination of whether the incident involves the impermissible use or disclosure of PHI; (2) a determination of whether the incident poses a significant risk of financial, reputational or other harm to the individual (the rules describe this element as a "risk assessment"); and (3) a determination of whether the incident falls under an exception. These breach determination reviews should be documented and retained for six years following the incident.

What are the exceptions? The rules identify several exceptions - no breach occurs if the incident involves: (1) the unintentional acquisition, access or use of PHI by a workforce member acting under the authority of a covered entity or business associate; (2) the inadvertent disclosure of PHI from one individual authorized to access PHI at the covered entity or a business associate to another individual authorized to access PHI at the covered entity or a business associate; (3) the unauthorized disclosure of PHI to an individual who would not reasonably have the opportunity to retain the information; or (4) a use or disclosure of PHI that does not include an individual's date of birth, zip code or any of the HIPAA identifiers.

When is a breach discovered? A breach is "discovered" on the first day the breach is known to the covered entity, or would have been known if the entity had exercised reasonable diligence. The date of discovery is important, because it starts the notice clock running (see notice requirements for individuals below). A covered entity is deemed to have knowledge of a breach if a member of the entity's workforce (other than the person responsible for the incident) knows of the breach or would have known of the breach if the person had exercised reasonable diligence. If a breach is discovered by a business associate who is an independent contractor, then the covered entity is not treated as discovering the breach until it receives notice from the business associate.

What are the requirements for providing notices to individuals? Following the discovery of a breach of unsecured PHI, the covered entity is required to provide a breach notice to affected individuals. The breach notice procedures for individuals include the following elements:

- Timing - A covered entity is required to notify affected individuals (or their personal representatives) as soon as reasonably possible, but in no event later than 60 calendar days after the breach is discovered. This time period is extended only if law enforcement authorities request a delay.

- Form and Method of Delivery - The notice must be in writing, and must be written in plain language. The notice must be sent by first class mail to the individual's last known address (or to the last known address of a personal representative), and may be sent by email if the individual has agreed to receive breach notices by email. If the address information is not known, a

substitute form of notice reasonably calculated to reach the individual must be provided (such as by conspicuous posting on the covered entity's web site or in major print or broadcast media accompanied by a toll-free phone number that remains active for at least 90 days).

- Content - The notice must include: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if those dates are known; (2) a description of the types of unsecured PHI involved in the breach (such as name, social security number, date of birth, home address, diagnosis codes); (3) a description of the steps 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, to mitigate harm to individuals and to protect against further breaches; and (5) contact procedures for individuals to ask questions or learn additional information (these procedures must include either a toll-free telephone number, an email address, a web site or a postal address).

What are the requirements for providing notices to HHS? Following the discovery of a breach of unsecured PHI that involves 500 or more individuals, a covered entity is required to provide a breach notice to HHS. The notice to HHS must be sent at the same time the covered entity provides notice to the affected individuals. If the breach of unsecured PHI involves less than 500 individuals, the covered entity is required to maintain a log or other documentation of the breach and submit that information to HHS no later than 60 days after the end of each calendar year. Additional information will be provided on the HHS web site.

What are the requirements for providing notices to prominent media outlets? Following the discovery of a breach of unsecured PHI that involves more than 500 residents of a single State or other jurisdiction (such as a county, city or town), a covered entity must provide a breach notice to prominent media outlets in that State or jurisdiction. The notice must be provided without unreasonable delay and in no case later than 60 days after the discovery of the breach. The notice to prominent media outlets must include the same content as the notice provided to individuals. The term "prominent media outlet" is not defined, but the preamble to the regulations suggests that the determination of major media outlets will vary depending on the state and the areas in which the affected individuals reside (major television stations or newspapers are listed as examples).

What are the obligations of business associates? A business associate is required to notify a covered entity when it discovers a breach of unsecured PHI relating to that covered entity. The business associate is not required to provide breach notices to individuals, HHS or prominent media outlets, unless it agrees to do so contractually. If the business associate is an agent, then the covered entity must provide the breach notice to individuals as soon as reasonably possible but no later than 60 days after the business associate discovered the breach. If the business associate is an independent contractor (which is typically the case for employer-sponsored health plans), then the covered entity must provide the breach notice to individuals as soon as reasonably possible but no later than 60 days after the business associate notifies the covered entity of the breach.

What other administrative requirements are imposed on covered entities? Covered entities are required to integrate the new breach notice rules into the following components of their HIPAA administrative infrastructure: (1) the entity's HIPAA policies and procedures; (2) the entity's HIPAA training process; (3) the entity's process for applying sanctions for HIPAA violations; and (4) the entity's HIPAA complaint process. In addition, a covered entity may not take retaliatory action against an individual who exercises a breach notice right, and may not require individuals to waive their breach notice rights. Although the regulations do not require covered entities to modify their privacy notices to reflect the breach notice rules, many covered entities may choose to do so.

What penalties apply to violations of the breach notice rules? Beginning in the near future, HHS will have the authority to apply the HIPAA civil and criminal penalties to violations of the breach notice rules. The HIPAA civil penalties, as expanded by ARRA, give HHS discretion to impose tiered monetary penalties based on the nature and extent of the violation and the resulting harm. The minimum and maximum penalty amounts increase depending on whether a covered entity knew about the violation, whether the violation was due to reasonable cause or whether the violation was due to willful neglect (and if due to willful neglect, whether and how quickly the violation was corrected). The following table summarizes the minimum and maximum HIPAA civil penalties that can be assessed:

Type of violation	Minimum penalty	Maximum penalty
Unknown violations (covered entity did not know of violation and would not have known even by exercising reasonable diligence)	$100 per violation, up to $25,000 per year for all violations of same requirement	$50,000 per violation, up to a maximum of $1.5 million per year for all violations of same requirement
Violations due to reasonable cause but not willful neglect	$1,000 per violation, up to $100,000 per year for all violations of same requirement	$50,000 per violation, up to a maximum of $1.5 million per year for all violations of same requirement
Violations due to willful neglect that are corrected within 30 days	$10,000 per violation, up to $250,000 per year for all violations of same requirement	$50,000 per violation, up to a maximum of $1.5 million per year for all violations of same requirement
Violations due to willful neglect that are not corrected within 30 days	$50,000 per violation, up to $1.5 million per year for all violations of same requirement	No maximum

The HIPAA criminal penalties apply to intentional violations and include both significant fines and possible imprisonment.

What steps should our health plan take to comply with the breach notice rules? At a minimum, your health plan should consider the following compliance actions:

- Review and revise business associate agreements - Your existing business associate agreements probably include provisions requiring a business associate to notify your health plan of HIPAA privacy and security violations. These provisions should be reviewed and revised as necessary to ensure

that the business associate notifies your plan of any breach incidents, and provides you with all the relevant information you need to conduct incident reviews and include in any breach notices that must be sent. You may also want to consider outsourcing your plan's breach notice requirements to one or more business associates.

- Inventory secured and unsecured PHI - The breach notice rules apply only to unsecured PHI. As a preliminary step, your plan may want to consider conducting an inventory of secured and unsecured PHI and reviewing approaches for securing PHI that is presently not secured. It may not be practical to encrypt or destroy all PHI, but conducting the inventory will allow you to determine whether additional forms of PHI may be secured.

- Establish an incident review procedure - The breach notice rules require your plan to review possible breach incidents. These reviews could be conducted by a single individual (such as the privacy or security official) or by a group of individuals (such as a committee). The review procedure should determine whether there has been an impermissible use or disclosure of PHI, whether there is a significant risk of financial, reputational or other harm to the individual, and whether the incident falls under one of the regulatory exceptions. These reviews should be documented in writing and retained for six years to protect the plan from audit or litigation risks.

- Establish appropriate notice procedures - The breach notice rules require your plan to issue timely and complete notices following the discovery of a breach of unsecured PHI. You should anticipate that breaches will occur, and develop appropriate procedures to ensure that notices to individuals and HHS (and prominent media outlets if applicable) can be issued as soon as reasonably possible and in no event later than 60 days following discovery of the breach. You may want to consider asking plan participants if they are willing to accept breach notices by email. You do not need to develop a sample form of notice, but doing so now may save time later.

- Revise HIPAA administrative infrastructure - The breach notice rules require your health plan to revise various elements of the plan's HIPAA administrative infrastructure. At a minimum, you should revise your HIPAA policies and procedures (to reflect both the incident review and notice procedures described above), revise your HIPAA training materials, revise your sanctions for HIPAA violations, and revise your HIPAA complaint process. When revising your HIPAA policies and procedures, you should also clarify that the plan will not take adverse action against an individual who questions your breach notice procedures, nor will you ask individuals to waive a breach notice to which they are entitled. The breach notice rules do not require you to revise your plan's HIPAA privacy notice, but you may want to consider doing so.

Please do not hesitate to contact SBA with any questions or if you require additional information.

Our special thanks to Chip Kerby of Liberté Group LLC for drafting content. Chip can be reached at 202-756-2459 or chip@libertegroup.com.

[1] See NIST Special Publications 800-111, 800-52, 800-77 and 800-113.
[2] See NIST Special Publication 800-88.

Strategic Benefits Advisors Inc.

Phone: 508-485-4000

Mark Abate- mark.abate@strategicba.com ext. 202

Mike Deneen- michael.deneen@strategicba.com ext. 203

Theresa Flynn- theresa.flynn@strategicba.com ext. 205

Lynn Gillis- lynn.gillis@strategicba.com ext. 206

David Hoffmann- david.hoffmann@strategicba.com ext. 204

Debbie Winer- debbie.winer@strategicba.com ext. 207