Coppersmith Schermer & Brockelman PLC

HHS Issues Breach Reporting Regulations under the HITECH Act
Executive Summary

The Health Information Technology for Economic and Clinical Health Act (the HITECH Act), which became law in February of this year as part of the stimulus bill, made substantial changes to the HIPAA Privacy and Security Rules, including:

- Establishing mandatory federal breach reporting requirements for HIPAA covered entities and their business associates;
- Applying many of the HIPAA privacy and security requirements directly to business associates;
- Creating new privacy requirements for HIPAA covered entities and their business associates; and
- Establishing new criminal and civil penalties for noncompliance and new enforcement authorities.

On August 24, 2009, the Department of Health and Human Services (HHS) published regulations implementing the HITECH Act federal breach reporting requirements. These regulations impose rigorous requirements to notify patients (and sometimes the media and HHS) of breaches of unsecured protected heath information, where those breaches pose a significant risk of financial, reputational or other harm to patients.

While the regulations are effective on September 23, 2009, HHS stated that it will exercise "enforcement discretion" and not impose penalties until February 22, 2010 to allow sufficient time for covered entities and business associates to come into full compliance with these new regulations. However, HHS expects covered entities to comply starting in September, and will work with them through technical assistance and voluntary corrective action to achieve compliance in the short term.

Next steps:

- *Determine whether and how the organization will "secure" its PHI*: Determine whether and how the organization will meet the encryption standards.
- *Implement policies*: Assemble a team to get the required policies and procedures in place to identify and respond to breaches of PHI.
- *Train your workforce*: Train your workforce on your policies.
- *Decide how you will deal with business associates:* Decide whether you will educate your business associates about their obligations, amend your business associate agreements to contain express reporting requirements, or both.
- *Respond promptly to possible breaches*: Respond immediately to any information about a potential breach within your organization or at a business associate.

The HITECH Act and the new HHS regulations require HIPAA covered entities and their business associates to report "breaches" of "unsecured" protected health information (PHI).

Section 13402 of the HITECH Act (42 U.S.C. § 17932) created a new federal breach reporting requirement for HIPAA covered entities and their business associates. The Act requires a covered entity that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses **unsecured protected health information**" to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such **breach**." Business associates are required to notify covered entities of breaches at the business associate.

On August 24, 2009, the Department of Health and Human Services (HHS) published regulations implementing the HITECH breach reporting requirements, providing more details on what constitutes "unsecured PHI" and what is a "breach."[1]

What is "unsecured" PHI? Section 13402(h) of the Act defined this term as PHI that is not secured through the use of a technology or methodology that renders PHI "unusable, unreadable, or indecipherable to unauthorized individuals," as specified by HHS guidance. HHS issued this guidance on April 17, 2009.[2] The Preamble to the HHS breach reporting regulations updated this guidance.[3]

The August 24th guidance specified two methods of securing information: (1) encryption in compliance with National Institute of Standards and Technology standards; or (2) destruction. In this revised guidance, HHS explained:

> a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by 'the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key' and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.[4] The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

---

[1] 74 Fed. Reg. 42740 (Aug. 24, 2009), *codified at* 45 C.F.R. Part 164, Subpart D.
[2] See http://snipr.com/g3wnv; 74 Fed. Reg. 19006 (Apr. 27, 2009) (date of publication in the Federal Register).
[3] 74 Fed. Reg. at 42741-43.
[4] The new guidance added that decryption tools should be stored separately from the encrypted data. The guidance on encryption is otherwise identical to the April 17 guidance.

i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.[5]
ii) Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, or others which are Federal Information Processing Standards FIPS 140-2 validated.[6]

b) The media on which the PHI is stored or recorded have been destroyed in one of the following ways:

i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.[7]
ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*,[8] such that the PHI cannot be retrieved.

If a covered entity or business associate encrypts or destroys its PHI consistent with this HHS guidance, then its information is "secure" and any breach would not be reportable under the HITECH Act. HHS is required to update its guidance annually, which it will post on its website.

Note that these regulations do not require encryption of PHI.[9] Rather, if covered entities and business associates encrypt PHI under the NIST guidelines, they will have "secured" the PHI and any breach of that information would not be reportable under the HITECH Act.

What is a "breach" of PHI? Section 13400 of the Act defined breach as follows:

> In general.--The term "breach" means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

---

[5] Available at http://www.csrc.nist.gov/.
[6] *Id.*
[7] The revised guidance clarified that redacting information does not make it "secure" for the reporting safe harbor.
[8] Available at http://www.csrc.nist.gov/.
[9] Under the HIPAA Security Rules, encryption of data is an "addressable implementation specification," which covered entities may decide not to implement if they use comparable methods to safeguard the PHI. *See* 45 C.F.R. § 164.312(a)(2)(iv) and (e)(2)(ii).

The HHS regulations first explained that the "unauthorized acquisition, access, use or disclosure" of PHI means a use or disclosure that is not permitted by the HIPAA Privacy Rule.[10] So, the first step in determining whether there has been a reportable breach is to determine whether a use or disclosure of PHI violated the HIPAA Privacy Rule.

Importantly, the HHS regulations also explained that a use or disclosure "compromises the security or privacy" of PHI only if it poses a significant risk of financial, reputational, or other harm to the individual."[11] This regulatory interpretation significantly reduces the negative impact of the federal breach reporting statute, as HHS chose not to adopt a "strict liability" reporting standard. HHS explained that, without a harm threshold, it was concerned that notification of every non-permitted use or disclosure would diminish the impact of notifications, cause unwarranted panic in individuals, and cause unnecessary expenditure of undue costs and other resources.[12] HHS also explained that having a harm threshold for reporting made the federal rules more consistent with most state breach reporting laws.[13]

In making a determination of whether there is a significant risk of harm to an individual whose PHI was used or disclosed in violation of the HIPAA Privacy Rule, HHS explained that covered entities and business associates should consider a number of factors, such as who used the information or to whom it was disclosed; the type and amount of PHI disclosed; and whether the entity took immediate steps to mitigate harm to individuals. In fact, the Preamble to the breach reporting regulations provided a number of helpful examples to understand when the use or disclosure of PHI may not pose a significant risk of harm to the individual:

- If PHI is impermissibly disclosed to a HIPAA covered entity or to a federal agency that must comply with the Federal Privacy Act, "there may be less risk of harm to the individual, since the recipient entity is obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information."[14]

- "[W]here a covered entity takes immediate steps to mitigate an impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed" this may reduce the risk.[15]

- If PHI is returned before being accessed for an improper purpose, such where forensic analysis of a recovered stolen laptop shows that information on the computer was not opened, altered, transferred or otherwise compromised, the temporary loss of the laptop may not pose a significant risk. However, HHS counseled that "if a computer is lost or

[10] 45 C.F.R. § 164.402.
[11] 45 C.F.R. § 164.402(1)(i).
[12] 74 Fed. Reg. at 42744.
[13] *Id.*
[14] *Id.*
[15] *Id.*

stolen, we do not consider it reasonable to delay breach notification based on the hope that the computer will be recovered."[16]

- The nature of the information inappropriately released may not pose a risk to the individual. For example, the release of only the name of an individual may not pose a risk, unless it is associated with an entity or physician providing sensitive types of services that may pose a reputational risk to the individual, such as substance abuse, mental health, or sexually transmitted disease treatment. HHS notes that inclusion of social security number, account number and a mother's maiden name may increase the risk of identity theft to individuals.[17]

This risk assessment will necessarily be a fact-specific determination. This lack of a black and white rule—while beneficial in that HHS did not impose "strict liability" reporting for all HIPAA Privacy Rule violations—will at the same time be a challenge for covered entities and their business associates in determining whether there is a reportable breach.

What are the exceptions to reporting a breach of unsecured PHI? The HHS regulations provided that a breach does not include the following types of uses or disclosures of unsecured PHI:

(1) The disclosure of a "limited data set" under HIPAA is not a breach unless the information includes date of birth or zip code.[18] A limited data set is partially de-identified data that may be used or disclosed for research, public health and health care operations purposes (such as a quality assurance), as long as the recipient signs a data use agreement that complies with the regulatory requirements.[19] A limited data set excludes the following "direct identifiers":

- Name;
- Postal address information, other than town or city, State, and zip code;
- Telephone numbers and fax numbers;
- Electronic mail addresses, URLs and Internet Protocol (IP) addresses;
- Social security numbers;
- Medical record numbers and health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

---

[16] 74 Fed. Reg. at 42745.
[17] *Id*.
[18] 45 C.F.R. § 164.402(1)(ii) (a "use or disclosure of [PHI] that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the [PHI]").
[19] 45 C.F.R. § 164514(e).

Even though these "direct identifiers" do not include dates related to a patient (such as birth date) or postal address above the street level address (such as zip code), HHS concluded that both date of birth and zip code pose a greater risk of harm if released, because those items can be used to re-identify information when paired with publicly available data.[20] Therefore, if any of the direct identifiers listed above, date of birth, or zip code is included in PHI that is used or disclosed in violation of the HIPAA Privacy Rule, it would not fall into this reporting exception and would be subject to the risk assessment process to determine whether reporting is necessary.

(2) The "unintentional acquisition, access, or use of [PHI] by a workforce member or person acting under the authority of a covered entity or a business associate" is not a breach "if the acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure" that violates the HIPAA Privacy Rule.[21] Workforce members include "employees, volunteers, trainees and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."[22] If a business associate is under the direct control of the covered entity (versus an independent contractor), this standard would include the use or disclosure of PHI by the business associate.

As an example of how this exception would apply, HHS explained that a billing employee's receipt of an email containing patient PHI mistakenly sent by a nurse would not be a breach if the billing employee notifies the nurse about the misdirected email and deletes the email. We anticipate that HHS would similarly interpret an employee mistakenly entering a patient's electronic health record, who then closes the record when the employee realizes the mistake. However, HHS noted that "curiosity viewing" would not be included in this exception: if "a receptionist at a covered entity who is not authorized to access [PHI] decides to look through patient files in order to learn of a friend's treatment … the impermissible access to [PHI] would not fall within this exception to breach because such access was neither unintentional, done in good faith, nor within the scope of authority."[23]

(3) A breach excludes "[a]ny inadvertent disclosure by an individual who is authorized to access [PHI] at a covered entity or business associate to another person authorized to access [PHI] at the same covered entity or business associate, or organized health care arrangement [OHCA] in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed" in violation of the HIPAA Privacy Rule.[24] Under this exception, if the recipient is an individual within the covered entity or business associate, or within an entity participating in an OHCA with the covered entity, and that individual is authorized to access PHI in his or her role, it is

[20] 74 Fed. Reg. at 42745-46.
[21] 45 C.F.R. § 164.402(2)(i).
[22] 45 C.F.R. § 160.103.
[23] 74 Fed. Reg. at 42747.
[24] 45 C.F.R. § 164.402(2)(ii).

not a breach as long as there isn't a further violation of the rules. (The release of PHI within a single entity has always been treated as a "use" under the HIPAA Privacy Rule, rather than a disclosure, but that technicality should not make a difference to the analysis.)

How would this "within the covered entity disclosure" apply in the context of a hospital system that maintains multiple hospitals or other provider sites? If a hospital system has declared its legal entities to be part of an "affiliated covered entity" under HIPAA,[25] then the different legal entities are treated as one entity for HIPAA compliance purposes. This exception would thus apply to disclosures between legal entities that are part of the affiliated covered entity. However, if a hospital system owns separate legal entities that are not part of an affiliated covered entity, then a disclosure between those entities that violates the HIPAA Privacy Rule would not fall within this exception.

How would this apply to disclosures among participants in an OHCA, such as a hospital and its medical staff?[26] Disclosures between OHCA participants will not be reportable—such as a physician's remote access to the wrong patient's hospital records—as long as the recipient does not further violate the HIPAA Privacy Rule in using or disclosing that patient's PHI.

(4) A disclosure of PHI where a covered entity or business associate has a good faith belief that a recipient of PHI would not reasonably have been able to retain the PHI, is not a breach.[27] HHS gave a few examples of what types of disclosure would fall within this exception:

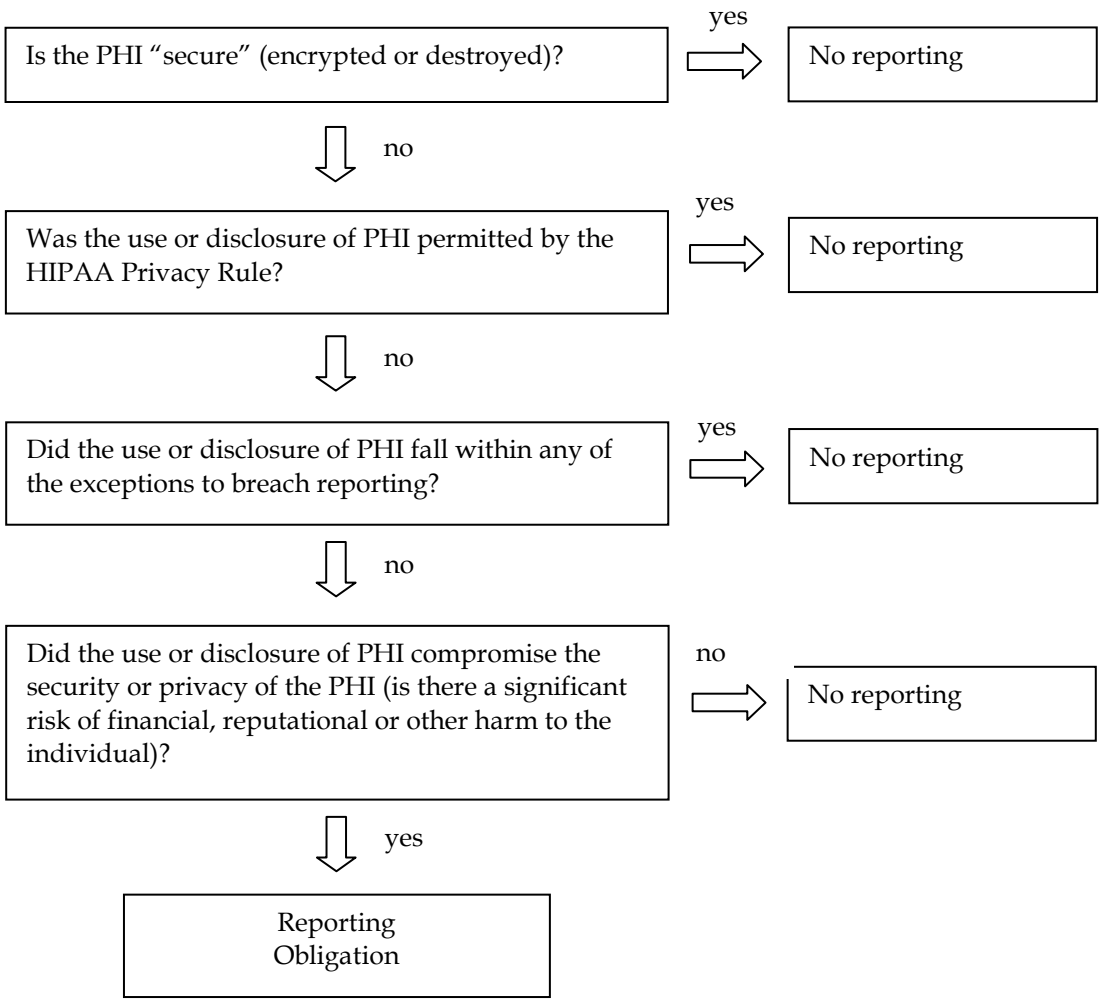
- If a covered entity sends an explanation of benefits form to the wrong person, and the EOB is return unopened as undeliverable, the covered entity can conclude that the improper addressee could not reasonably have retained the information.

- If a nurse mistakenly provides discharge instructions to the wrong patient, quickly realizes the mistake, and recovers the instructions to provide to the correct patient, this would not constitute a breach if "the nurse can reasonably conclude that the patient could not have read or retained the information."[28]

What analysis should covered entities use to determine whether they have a reporting obligation? In summary, to determine whether reporting is required under the HHS regulations, we suggest a covered entity use the following analysis:

---

[25] 45 C.F.R. § 164.105.
[26] 45 C.F.R. § 160.103 (defining an OHCA as a "clinically integrated care setting in which individuals typically receive health are from more than one health care provider," among other arrangements).
[27] 45 C.F.R. § 164.402(2)(iii).
[28] 74 Fed. Reg. at 42748.



What are the notice requirements? If there is a reportable breach, the Act and the HHS regulations contain the same rigorous notification requirements:

- *Individuals notified; timing*: Covered entities must notify "each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach" without unreasonable delay and in no case later than 60 days of discovery of the breach by the covered entity (unless there is a law enforcement request for delay).[29]

  A breach is discovered on the first day the *incident* becomes known by the covered entity, not when the covered entity concludes that, under the risk analysis described above, there has been a breach that is reportable.[30] An incident is known when the covered entity has knowledge of the incident, or by exercising reasonable diligence

[29] 45 C.F.R. § 164.404(a).
[30] 74 Fed. Reg. at 42749.

should have known of the incident.[31] This applies if a workforce member or an "agent" (under the federal common law of agency) of the covered entity knows of the incident—unless that person committed the breach. [32] This puts a premium on good procedures to identify a breach and to quickly determine whether reporting is required.

The only time notice may be delayed is if a law enforcement official represents that notice would impede a criminal investigation or cause damage to national security.[33] If the law enforcement official provides a statement to that effect in writing, the delay may be for the period of time specified by the official; if the representation is oral, the delay may last no longer than 30 days unless a written statement is received (and the official's statement must be documented, including the identity of the official).[34]

- *Manner and form of notice*: Notice must be made by first-class mail (or email if specified by an individual). If there is insufficient or out-of-date contact information, a covered entity must do a "substitute form of notice" such as telephone notice or other means. If there are more than 10 individuals for whom the covered entity has insufficient contact information, the entity must do a conspicuous website posting for at least 90 days, or conspicuous notice in major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside. This notice must include a toll-free number that is active for at least 90 days, so that individual may call to determine if their PHI was involved in the breach. The entity may also provide information by telephone or other means—in addition to the written notice—if an urgent situation where possible misuse of the PHI is imminent, but there is no obligation to do so.[35]

- *Notice to the media:* If more than 500 residents of a State or jurisdiction are involved, the entity must provide notice to "prominent media outlets" serving that State or jurisdiction.[36]

- *Self-disclosure to HHS*: If more than 500 residents are involved, the entity must provide notice to HHS at the same time the notice is required to affected individuals. If fewer than 500 residents are involved, the entity must log the breach and disclose it to HHS in an annual report by March 1 every year (60 days after the end of each calendar year), in a manner that will be specified on the HHS website.[37]

- *Content of notice*: The notice to individuals must contain a description of what happened (including the date of the breach and the date of discovery of the breach, if known), a description of the *types* of unsecured PHI involved (such as name, social security number or date of birth), the steps individuals should take to protect themselves from

---

[31] 45 C.F.R. § 164.404(a)(2).
[32] *Id.*
[33] 45 C.F.R. § 164.412.
[34] *Id.*
[35] 45 C.F.R. § 164.404(a)(3).
[36] 45 C.F.R. § 164.406.
[37] 45 C.F.R. § 164.408.

potential harm (such as filing a fraud alert with the credit reporting agencies), a description of the covered entity efforts to investigate, mitigate and prevent further breaches, and contact information for individuals to ask questions and learn additional information , which must include a toll-free number, an email address, website or postal address.[38] The notice must be in plain language.[39]

How does this reporting requirement affect business associates? A business associate is not required to provide notice of the breach to the individual, but instead must notify the covered entity. The business associate must include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate, to have been used or disclosed during the breach (if that information is known), along with any other available information the business associate has that the covered entity will be required to include in the notice to the individual.[40]

The same content and timing requirements apply to business associates: they must provide notice to the covered entity without unreasonable delay and in no case later than 60 calendar days after the business associate's discovery of the breach.[41] Note however, that if the business associate is acting as an "agent" of the covered entity under the federal common law of agency, the business associate's discovery of the breach will be imputed to the covered entity; covered entities thus should consider requiring their business associates to report to the covered entity within a time period shorter than 60 days.

Who has the burden of proof to demonstrate that the required reporting occurred? Covered entities and business associates have the burden of proof of demonstrating why breach notification was not required.[42] All of the documentation related to the decision of whether or not to report, the timing of that report, and to whom reporting was made, should be retained for six years.

What administrative requirements do the HHS regulations impose? Both covered entities and business associates must comply with the administrative requirements listed at 45 C.F.R. §§ 164.530(b), (d), (e), (g), (h), (i) and (j).[43] These include:

- Policies and procedures to implement this rule;
- Training to all workforce members on those policies and procedures, if necessary to the workforce members' functions;
- A process for individuals to complain about the entity's policies and procedures, or compliance with those policies;
- A process for applying sanctions against workforce members who fail to comply with the entity's policies and procedures;

---

[38] 45 C.F.R. § 164.404(c).
[39] *Id*.
[40] 45 C.F.R. § 164.410.
[41] *Id*.
[42] 45 C.F.R. § 164.414(b).
[43] 45 C.F.R. § 164.414(a).

- A prohibition against intimidating or retaliatory acts for the exercise of the individual's right to complain;
- A prohibition against requiring individuals to waive their rights as a condition of receiving treatment, payment, enrollment, or eligibility in a health plan; and
- Retention of policies and procedures and any activity that must be documented, for a period of six years.

What is the effective date of the HHS regulations? Covered entities and business associates must comply with these regulations by September 23, 2009, thirty days after they were published in the Federal Register. However, HHS will exercise its "enforcement discretion" and will not impose penalties until February 22, 2010 to allow covered entities and business associates sufficient time to determine how to secure (encrypt) PHI if they choose to do so, to work on their systems to detect breaches, to implement their policies and processes for responding to breaches of protected health information, and to train their workforce members.[44] Moreover, HHS noted some ambiguity in the statute regarding whether HHS may enforce the regulations against business associates before February 18, 2010.[45]

Keep in mind, however, that if a reportable breach happens between September 23, 2009 and February 22, 2010, covered entities and business associate are still required to follow the reporting requirements. If there is a violation between these dates, HHS will work with covered entities and business associates through technical assistance and voluntary corrective action to achieve compliance. Moreover, it *possible* that State Attorneys General will be able to enforce the regulations—at least against covered entities—after September 23.

Do state security breach reporting statutes continue to apply? Yes, most state security breach reporting statutes continue to apply. Section 13421 of the Act (42 U.S.C. § 17951) applies the HIPAA state law preemption standards found at 42 U.S.C. § 1320d-7. This means that the HHS breach reporting regulations supersede any "contrary" provision of state law, which would apply only if it is impossible to comply with both the federal and state reporting requirements or if the state requirement "stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of the federal breach notification provisions. This is unlikely to occur, as the covered entity or business associate would simply comply with the stricter requirements imposed, such as following the law that requires faster notice or more information in the notice.[46]

---

[44] 74 Fed. Reg. at 42756.

[45] *Id.*

[46] By way of example, Arizona's security breach reporting statute would not be preempted by the HHS regulations. While Arizona Revised Statutes § 44-7501 expressly exempts HIPAA covered entities from its application, it requires other businesses (including business associates) to notify an individual of the unauthorized acquisition and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of the individual's personal information (which includes name in combination with social security number, drivers license or identification number, or financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account). It is possible for Arizona businesses to comply with both the Arizona statute and the HHS regulations.

What penalties apply if a covered entity or business associate fails to follow the HHS breach reporting regulations? The HITECH Act created a "tiered" system of penalties:

- *If the person did not know (and by exercising reasonable diligence would not have known) that such person violated a provision*, the civil penalty is between $100 - $50,000 for each violation, up to a total of $25,000-$1,500,000 per year for all violations of an identical requirement;

- *If the violation was due to reasonable cause and not to willful neglect*, the civil penalty is between $1,000 - $50,000 for each violation, up to a total of $100,000-$1,500,000 per year for all violations of an identical requirement;

- *If the violation was due to willful neglect*, the civil penalty is between $10,000 - $50,000 for each violation, up to a total of $250,000-$1,500,000 per year for all violations of an identical requirement if the violation was corrected during the 30 day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred. If the violation is not corrected within 30 days, the penalties increase to $50,000 for each violation, up to a total of $1,500,000 per year for all violations of an identical requirement.

Because HHS is exercising "enforcement discretion," it will not impose these enforcement penalties for the failure to follow the HHS breach reporting regulations until February 22, 2010.

However, keep in mind that Section 13410(e) of the HITECH Act gave enforcement authority to State Attorneys General to enforce the HIPAA Privacy and Security Rules, where an Attorney General has "reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates a provision of this part." State Attorneys General are authorized to bring a civil action to enjoin a violation or to obtain statutory damages on behalf of those residents. These statutory damages are calculated by multiplying the number of violations by $100, up to $25,000 for violations of each identical requirement. The Act also permits states to seek the award of attorneys' fees.

Because the federal breach reporting regulations are effective on September 23, 2009, they may be enforceable by the State Attorneys General on that date, even though HHS will itself not enforce these regulations until February 2010. We certainly hope that State Attorneys General across the country will similarly decline to enforce these new regulations for a sufficient period of time to enable covered entities and business associates to implement their new policies and train workforce members.

Do the new FTC regulations apply to HIPAA covered entities and their business associates? The HITECH Act required vendors of personal health records (PHR), entities that provide products or services through the website of PHR vendors, and entities that access or send information to a PHR, to notify each citizen or resident of the United States of a breach of security where "unsecured PHR identifiable information" was acquired by an unauthorized

person as a result of the breach.[47] The Federal Trade Commission published final regulations to implement this part of the HITECH Act on August 25, 2009.[48] The FTC regulations do not apply to HIPAA covered entities or to entities acting in their capacity as business associates. The FTC regulations would apply to business associates if they are PHR vendors or the other categories of entities covered by the regulations, while not acting in their capacity as business associates.

For any questions about the HITECH Act or these breach reporting regulations, please contact Kristen Rosati at 602-381-5464 or krosati@csblaw.com or other members of the CSB Health Care Law Group.

The CSB Health Care Law Group
Beth Schermer: 602.381.5462, bschermer@csblaw.com
Karen Owens: 602.381.5463, kowens@csblaw.com
Julie Nelson: 602.381.5465, jnelson@csblaw.com
Kristen Rosati : 602.381.5464, krosati@csblaw.com
Joel Wakefield : 602.381.5480, jwakefield@csblaw.com
Mayan Tahan: 602.381.5475, mtahan@csblaw.com

---

[47] Section 13407 (42 U.S.C. § 17937).
[48] *See* 74 Fed. Reg. 42962 (Aug. 25, 2009), *codified at* 16 C.F.R. § Part 318. *See also* FTC Web site for more information at http://www2.ftc.gov/opa/2009/08/hbn.shtm.