HIPAA Regulations: Notification in the Case of Breach -- Notification to the Media - § 164.406

As Contained in the HHS Rules on Notification in the Case of Breach of Unsecured Protected Health Information

HHS Regulations as Amended January 2013
Notification in the Case of Breach -- Notification to the Media - § 164.406

(a) *Standard.* For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.

(b) *Implementation specification: Timeliness of notification.* Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* The notification required by paragraph (a) of this section shall meet the requirements of §164.404(c).

HHS Description and Commentary From the January 2013 Amendments
Notification in the Case of Breach -- Notification to the Media - § 164.406

Section 13402(e)(2) of the HITECH Act, implemented at § 164.406 of the interim final rule, requires that a covered entity provide notice of a breach to prominent media outlets serving a State or jurisdiction, following the discovery of a breach if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. This media notice is in addition to, not a substitute for, individual notice. In accordance with the Act, § 164.406(b) of the interim final rule required covered entities to notify prominent media outlets without unreasonable delay and in no

HIPAA Regulations: Notification in the Case of Breach -- Notification to the Media - § 164.406

Section 164.406(c) of the interim final rule required that the notification to the media include the same information required to be included in the notification to the individual under § 164.404(c).

The interim final rule did not define "prominent media outlet" because what constitutes a prominent media outlet will differ depending upon the State or jurisdiction affected. For a breach affecting more than 500 individuals across a particular state, a prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sports or politics) would not be viewed as a prominent media outlet. Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, then a prominent media outlet may be a major, general-interest newspaper with daily circulation throughout the city, even though the newspaper does not serve the whole State.

With regard to the term "State," the existing definition of "State" at § 160.103 of the HIPAA Rules applies. Section § 160.103 defines "State" to mean "any one of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam." We also expressly provided in the regulation that "State" for purposes of notice to the media includes American Samoa and the Northern Mariana Islands, because they were included in the HITECH Act's definition of "State" in addition to what appears in the definition at § 160.103. With respect to what was meant by "jurisdiction" as opposed to a "State," jurisdiction is a geographic area smaller than a state, such as a county, city, or town.

The interim final rule also clarified that some breaches involving more than 500 individuals who are residents in multiple States may not require notice to the media. For example, if a covered entity discovers a breach of 600 individuals, 200 of which reside in Virginia, 200 of which reside in Maryland, and 200 of which reside in the District of Columbia, the breach did not affect more than 500 residents of any one State or jurisdiction, and as such, notification is not required to be provided to the media pursuant to § 164.406. However, individual notification under §164.404 would be required, as would notification to the Secretary under § 164.408 because the breach involved 500 or more individuals.

The Department also recognized that in some cases a breach may occur at a business associate and involve the protected health information of multiple covered entities. In such cases, a covered entity involved would only be required to provide notification to the media if the information breached included the protected health information of more than 500 individuals located in any one State or jurisdiction. For example, if a business associate discovers a breach affecting 800 individuals in a State, the business associate must notify the appropriate covered entity (or covered entities) subject to § 164.410 (discussed below). If 450 of the affected individuals are patients of one covered entity and the remaining 350 are patients of another covered entity, because the breach has not affected more

HIPAA Regulations: Notification in the Case of Breach -- Notification to the Media - § 164.406

than 500 individuals at either covered entity, there is no obligation to provide notification to the media under this section.

Section 164.406(c) requires that the notice to the media include the same content as that required for notification to the individual under § 164.404(c), and we emphasized that this provision does not replace either direct written or substitute notice to the individual under §164.404.

Overview of Public Comments

In general, we received few comments on this provision of the interim final rule.

One commenter expressed general support for this provision because it does not require the covered entity to incur the cost of printing or running the media notice and asked for clarification that this policy places no requirement on the media to publically report the information provided by a covered entity. Another commenter asked whether a covered entity could fulfill the requirements for providing media notification by posting a press release on the covered entity's Web site.

Final Rule

We retain § 164.406 in this final rule with one minor change.

As described in Section IV above, to align the definition of "State" in the HIPAA Rules with the definition of the same term used in the HITECH Act, the Department has modified the definition of "State" at § 160.103 to include reference to American Samoa and the Northern Mariana Islands. Given this change, it is not necessary to include specific reference to American Samoa and the Northern Mariana Islands at § 164.406 and we remove it in this final rule.

In response to public comments, we clarify that § 164.406 does not require a covered entity to incur any cost to print or run media notice about a breach of unsecured protected health information (unlike the obligations for providing substitute notice to individuals in § 164.404(d)(2) if there is insufficient or out-of-date contact information for 10 or more affected individuals) nor does it obligate prominent media outlets who receive notification of a breach from a covered entity to print or run information about the breach. We also emphasize that posting a press release regarding a breach of unsecured protected health information on the home page of the covered entity's Web site will not fulfill the obligation to provide notice to the media (although covered entities are free to post a press release regarding a breach on their web site). To fulfill the obligation, notification, which may be in the form of a press release, must be provided directly to prominent media outlets serving the State or jurisdiction where the affected individuals reside. **HHS Description and Commentary From the Interim Breach Rule Notification in the Case of Breach -- Notification to the Media**

HIPAA Regulations: Notification in the Case of Breach -- Notification to the Media - § 164.406

Section 164.406 implements § 13402(e)(2) of the Act, which requires that notice be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. This media notice differs from the substitute media notice described in § 164.404(d)(1)(2) in that it is directed "to" the media and is intended to supplement, but not substitute for, individual notice. The Act requires that notification to the media under this provision be provided within the same timeframe as notice is to be provided to the individual. See § 13402(d)(1) of the Act. Accordingly, § 164.406(b) of the interim final rule requires a covered entity to notify prominent media outlets without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. In paragraph (c) of this section, we require that notification to the media under this provision include the same information required to be included in the notification to the individual under § 164.404(c). We expect that most covered entities will provide notification to the media under this section in the form of a press release.

Commenters asked that we define what constitutes a "prominent media outlet." We do not define "prominent media outlet" in this regulation because what constitutes a prominent media outlet will differ depending upon the State or jurisdiction affected. For example, for a breach affecting 500 or more individuals across a particular state, a prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sport, politics) would not be viewed as a prominent media outlet. If a breach affects 500 or more individuals in a limited jurisdiction, such as a city, then a prominent media outlet may be a major, general-interest newspaper with daily circulation throughout the city, even though the newspaper does not serve the whole State.

Commenters also asked HHS to clarify what is meant by "State or jurisdiction" for purposes of notice to the media under this provision. We note that "State" is already defined at § 160.103 of the HIPAA Rules to mean "any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam." That definition applies to this new provision. We also note that the Act includes a definition of "State" which applies for purposes of this provision and defines "State" to include, in addition to what is included at §160.103, American Samoa and the Northern Mariana Islands. Thus, we provide at §164.406(a) that, for purposes of this provision, "State" also includes American Samoa and the Northern Mariana Islands. With respect to jurisdiction, we clarify that, for purposes of this provision, jurisdiction is a geographic area smaller than a state, such as a county, city, or town.

To illustrate how these provisions apply, we provide the following example. If laptops containing the unsecured protected health information of more than 500 residents of a particular city were stolen from a covered entity, notification under this section should be provided to prominent media outlets serving

HIPAA Regulations: Notification in the Case of Breach -- Notification to the Media - § 164.406

that city. In this case, the prominent media outlet may be a major television station or newspaper (or other media outlet) serving primarily the residents of that city or a prominent media outlet serving the entire state. Alternatively, for a breach involving 500 or more residents across a State and not within any one particular county or city of the State, the prominent media outlet chosen must serve the entire State.

In response to comments received, we also offer clarification on how to address a breach involving residents in multiple States or jurisdictions. For example, if a covered entity discovers a breach of 600 individuals, 200 of which reside in Virginia, 200 of which reside in Maryland, and 200 of which reside in the District of Columbia, such a breach did not affect more than 500 residents of any one State or jurisdiction, and as such, notification is not required to be provided to the media pursuant to § 164.406.

However, individual notification under §164.404 would be required, as would notification to the Secretary under § 164.408 because the breach involved 500 or more individuals. Conversely, if a covered entity discovered a breach of unsecured protected health information involving 600 residents within the state of Maryland and 600 residents of the District of Columbia, notification must be provided to a prominent media outlet serving the state of Maryland and to a prominent media outlet serving the District of Columbia.

We also recognize that in some cases a breach may occur at a business associate and involve the protected health information of multiple covered entities. In that case, a covered entity involved would only be required to provide notification to the media if the information breached included the protected health information of 500 or more individuals located in any one State or jurisdiction. For example, if a business associate discovers a breach affecting 800 individuals, the business associate must notify the appropriate covered entity (or covered entities) subject to § 164.410 (discussed below).

If 450 of the affected individuals are patients of one covered entity and the remaining 350 are patients of another covered entity, because the breach has not affected more than 500 individuals at either covered entity, there is no obligation to provide notification to the media under this section. Additionally, neither covered entity has the obligation of notifying the Secretary under § 164.408(b) concurrently with notice to the affected individuals; however, both covered entities must include this breach in their annual submission to the Secretary pursuant to § 164.408(c). In cases where the entities involved are unable to determine which entity's protected health information was involved, the covered entities may consider having the business associate provide the notification to the media on behalf of all of the covered entities.

HIPAA Regulations: Notification in the Case of Breach -- Notification to the Media - § 164.406

Section 164.406(c) sets forth the content requirement for covered entities notifying the media. In this section, we require that the notice to the media include the same content as that required for notification to the individual under § 164.404(c). We emphasize that this provision does not replace either direct written or substitute notice to the individual under §164.404. If a covered entity is required to provide substitute notice under § 164.404(d)(2)(ii)(A) and chooses to do so through major print or broadcast media, notification to the media under this section would only satisfy such substitute notice if the prominent media outlet ran a notification reasonably calculated to reach the individuals for which substitute notice was required and included all the information required be provided in the individual notice, including the toll-free number required by § 164.404(d)(2)(ii)(B).