American Hospital Association

Liberty Place, Suite 700
325 Seventh Street, NW
Washington, DC 20004-2802
(202) 638-1100 Phone
www.aha.org

May 21, 2009

Kathleen Sebelius, Secretary
U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HITECH Breach Notification
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Re: Guidance and Request for Information -- Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009, 74 Fed. Reg. 19006 (April 27, 2009).

Dear Secretary Sebelius:

On behalf of our more than 5,000 member hospitals, health systems and other health care organizations, and our 40,000 individual members, the American Hospital Association (AHA) appreciates the opportunity to comment on the Department of Health and Human Services' (HHS) guidance on the technologies and methodologies that render protected health information (PHI) unusable, unreadable or indecipherable to unauthorized individuals (Guidance) published in the April 27 *Federal Register*.

Under the *Health Information Technology for Economic and Clinical Health (HITECH) Act* enacted in February as part of the economic stimulus package, entities covered by the *Health Insurance Portability and Accountability Act* (HIPAA), and their business associates, must notify affected individuals of a breach of their "unsecured" PHI. HITECH defines "unsecured PHI" as any PHI that is not secured through the use of a technology or methodology specified in guidance issued by the Secretary. While not required by the statute to use the technologies and methodologies in the Guidance, covered entities and their business associates that do so would not have to provide notice under federal law if a breach of PHI occurs. In effect, the use of these technologies and methodologies provides a "safe harbor" from HITECH's breach notification requirements.

America's hospitals are dedicated to safeguarding the privacy of their patients' medical information, and the AHA and its members support HHS' efforts to create a data breach

notification safe harbor. We generally endorse the proposed standards that will be used to identify "unsecured health information" that is subject to HITECH's breach notification provisions. However, we offer some suggestions for further improvements in the Guidance to ensure it effectively serves its purpose with respect to the breach notification requirements under HITECH, as well as recommendations about the breach notification provisions generally. Specifically, we urge HHS to:

- Include the limited data set, as specified in the Privacy Rule, as a methodology that puts data within the safe harbor from breach notification.
- Work with the Food and Drug Administration to address the protection of ePHI collected by, stored on and/or transmitted by medical devices.
- Explicitly provide that encrypting backup media with mechanisms substantially similar to those contained in NIST Special Publication 800-111 is an approved encryption mechanism for purposes of the breach notification requirements.
- Provide guidance that directly addresses the array of secure mechanisms available for the transmission of ePHI via e-mail as well as guidance on which methods of redaction covered entities and their business associates may use to appropriately secure PHI, especially paper PHI.
- Refrain from specifying which off-the-shelf products meet the encryption standards.

In anticipation of the forthcoming rulemaking on breach notification, we also recommend taking steps to minimize potential conflicts between the federal and existing state breach notification provisions, including recommendations related to preemption of state requirements under the HIPAA statute; eliminating the need for confusing and unnecessary breach notices for certain internal disclosures of PHI where no further inappropriate acquisition, access, use or disclosure occurs; and permitting the combination of state and federal notices to minimize anxiety and confusion among individuals who would otherwise receive two notice letters about the same incident.

Our detailed comments and recommendations on specific components of the Guidance, and the HITECH breach notification provisions generally, are attached.

The Guidance and the regulations are extremely important to both patients and providers, and we feel strongly that they must be workable and practical to be of enduring value. The AHA stands ready to assist HHS as it works to revise its Guidance on technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals and initiates the process for promulgating its interim final regulations on federal breach notification. If you have any questions about our comments and recommendations, please contact Lawrence Hughes, assistant general counsel, advocacy and public policy, at lhughes@aha.org or (202) 626-2346.

Sincerely,

Rick Pollack
Executive Vice President

AHA's Detailed Comments on
HHS' Guidance for Securing PHI and HITECH's Breach Notification Provisions Generally

I. Encryption Standards as a "Safe Harbor" from Breach Notification Requirements

The AHA supports the Department of Health and Human Services' (HHS) approach in establishing a data breach notification safe harbor for secured electronic protected health information (ePHI), and we agree that encrypted information should be considered to be within that safe harbor. However, we are acutely aware that many of our hospitals' data systems do not easily lend themselves to encryption. Accordingly, we encourage HHS to resist requests to create a de facto obligation that covered entities encrypt ePHI. Any such obligation would be inconsistent with the *Health Information Technology for Economic and Clinical Health (HITECH) Act's* plain text that creates a safe harbor from breach notification for entities that secure their PHI rather than establishing a new standard that would require those entities to secure that data.

Creating such an obligation also would materially change the *Health Insurance Portability and Accountability Act* (HIPAA) Security Rule in unworkable ways. The Security Rule provides that encryption of data at rest and data in motion is an "addressable specification," meaning that covered entities (and now business associates) may assess whether those specifications are reasonable and appropriate safeguards for the specific circumstances of that entity. (*See* 45 C.F.R. §§ 164.312(a)(2)(iv), (e)(2)(ii).) We agree with the approach taken in the Security Rule, which leaves the determination of whether to encrypt data at rest and data in motion to the entities covered by that Rule, and believe that this remains the appropriate conclusion that is consistent with the language and intent of the HITECH Act. **HHS should resist requests that it convert an element of the HITECH data breach notification provisions into a uniform requirement to encrypt ePHI.**

The Guidance's concept of establishing a "safe harbor" is particularly important given the challenges of encrypting certain types of data, and we encourage HHS to consider the significant challenges related to implementing encryption standards. Indeed, in many cases, encryption is not a workable option. For example, server networks in health care entities typically hold terabytes of ePHI that must be accessed and used without undue delay in providing health care services, including services delivered in time-sensitive, life-threatening situations. Encrypting that data would add notable delays to accessing, modifying, and saving changes to data, which in turn may lead to delays and confusion in providing health care to patients. It will increase the resources necessary to store existing data and, thus, will increase maintenance costs. For health care providers, encryption of live server PACS medical images also may introduce delays in patient care and onerous cost burdens to providers.

Encrypting data on storage area networks also may present significant key management difficulties. Ensuring proper key management in patient care environments may require

expenditures on new technology, staff training and additional IT staff management, whose costs could outweigh the value of added protections in hospital settings. An inability to manage keys properly given the urgency and intensity of information use by teams of professionals, such as those in a surgical suite or emergency room, also could undermine the purpose of encryption. If keys are not properly stored or escrowed, they may be compromised, which would render the encryption meaningless. On the other hand, improper key management also could compromise the provision of care. If keys are lost or misplaced, authorized users may not be able to decrypt important data when it is urgently needed for patient care.

Despite the challenges of encrypting certain types of data, particularly data at rest or in use on a large server network, the AHA supports HHS' proposal to consider encryption as a functional safe harbor for purposes of the breach notification requirement. Encryption is an important tool for covered entities and business associates in protecting certain types of data environments, but it is not a feasible standard for many types of data used and maintained by covered entities.

In particular, the use of encryption raises special issues in specific circumstances described below and providers would welcome additional guidance in these areas.

Application of Encryption Standards to Medical Devices. A wide variety of modern medical devices that are used in treatment settings collect, store and/or transmit ePHI. The application of the Guidance's encryption standards to these medical devices raises serious concern. Data encryption is not a common feature of medical devices, particularly legacy equipment; and many of these devices rely upon proprietary software that is controlled by the device manufacturers, who are not covered entities or business associates under HIPAA. Hospitals are not authorized to make custom changes to a Food and Drug Administration (FDA) approved medical device, and they have little power to compel device manufacturers to change their products to facilitate data encryption. Adding encryption technology would require substantial redesign of existing products and likely would be subject to the delay and cost of further FDA review and approval, and may not be possible at all for certain devices. Hospitals are not able to add encryption technologies themselves, and it would be difficult to convince device manufacturers to change their products if doing so required them to complete the FDA approval process again. Many hospitals, therefore, rely on physical and administrative safeguards to secure information retained within medical devices. **To the extent that HHS regards encryption and other technical standards as technologies or methodologies that covered entities should aspire to implement, we urge HHS to work with FDA to address the protection of ePHI collected by, stored on and/or transmitted by medical devices.**

Backup Media. Backup media are not addressed directly in the "data at rest" guidance. For example, tapes, flash memory and optical disks are not strictly end-user devices and, thus, are not technically covered by NIST Special Publication 800-111. While some of the mechanisms discussed in NIST Special Publication 800-111 are applicable to backup media, **it would be helpful if HHS would provide explicit assurance that encrypting backup media with mechanisms substantially similar to those contained in NIST Special Publication 800-111 would be an approved encryption mechanism and would be sufficient to render PHI**

unusable, unreadable or indecipherable to unauthorized individuals for purposes of the breach notification requirements.

Security of E-mail Messages. E-mail messages containing ePHI would appear to fall within the definition of "data in motion," but the NIST publications referenced in the Guidance do not specifically address e-mail. Transport Layer Security (TLS) may be applicable in some forms, particularly for webmail services, but restricting all covered entities and business associates to TLS would exclude alternatives such as Secure/Multipurpose Internet Mail Extensions (S/MIME), which operate on the application layer of the OSI Model rather than on the transport layer. The absence of clear guidance regarding security for e-mail messages containing ePHI may push covered entities and business associates to standardize software and hardware selections on the products that are FIPS 140-2 approved by the NIST Cryptographic Module Validation Program (CMVP). This would turn the CMVP into a de facto government-approved list of technologies for purchase by private entities. **We request that HHS instead provide guidance that directly addresses the array of secure mechanisms available for the transmission of ePHI via email.**

II. Methods to Render Paper PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

The AHA urges HHS to include redaction as an approved method of rendering PHI unusable, unreadable or indecipherable to unauthorized individuals. When properly carried out, we believe that redaction is an appropriate method for rendering PHI secured. Many HIPAA-covered entities and their business associates make only limited use (or no use) of information technology, and we believe that they should have access to a safe harbor for securing PHI in paper form. The AHA recognizes that not all methods of redaction are sufficient to render PHI unusable, unreadable or indecipherable to unauthorized individuals, so **we suggest that HHS consider issuing guidance on which methods of redaction covered entities and their business associates may use to appropriately secure PHI.**

III. Limited Data Sets

The AHA strongly endorses HHS' suggestion to treat PHI in the form of a limited data set (LDS) as unusable, unreadable or indecipherable to unauthorized individuals for purposes of breach notification. **It is critical that placing information in LDS format be considered a methodology that renders the PHI exempt from the breach notification rules.** Our reasons are rooted both in law and in practical considerations.

First, the policy underlying breach notification law is to inform individuals of an event that could have consequences to them, such as risk of identity theft. The data fields that are permitted to be included in an LDS are not data that would be useful for those illicit purposes, and are designed to make it extremely difficult, if not impossible, for the data to be used to identify or contact the individual. Accepting that an LDS is not "unsecured" information for purposes of breach notification would help make the HHS guidance and future federal regulations more compatible

with state breach notification laws, because those laws typically require notification only for breaches of information that includes certain direct identifiers.

Second, as a practical matter, it would be difficult, if not impossible, for covered entities to notify individuals of a breach of data in LDS form. Because the LDS does not contain direct identifiers and because covered entities often do not retain a method to re-identify the data in an LDS, it is entirely unclear that a hospital would be able to re-identify that data in order to notify the individuals allegedly affected by unauthorized access to an LDS. Indeed, authorized recipients of an LDS are accountable for limiting use and disclosure of the LDS under their Data Use Agreement with the covered entity, including safeguarding it from unauthorized users. The AHA believes there is little risk of re-identification of individuals whose data were used to create an LDS and, thus, the LDS criteria as specified in the Privacy Rule should be considered a methodology that puts data within the safe harbor from breach notification.

The AHA also believes that significant additional risk to patient privacy would be created by HHS' failure to provide a safe harbor for LDS data. At a minimum, such an action would mean that covered entities in the future will have to ensure that all such data in an LDS have a code that can be used to re-identify the patients and contact them in the event of a breach of the otherwise non-identifying information. This would have the troubling effect of both rendering the LDS less secure and creating anxiety and confusion among the notified individuals, who arguably would otherwise have little to be anxious about with respect to the LDS.

Finally, the AHA is deeply concerned that failure to establish a safe harbor for PHI in LDS form would create a strong disincentive for covered entities to use an LDS in the future. Because data in LDS form are so widely used for public health, quality improvement activities and other research, the lack of a safe harbor could have a chilling effect on these essential analyses. We urge HHS to consider the importance of encouraging use of the LDS for research and for health care operations analyses of quality, safety and efficiency in patient care as it considers the LDS issue. Certainly, in light of the policy objectives served by breach notification, it would be illogical for HHS to create a greater risk to privacy by failing to include LDS on its list of approved technologies and methodologies for rendering data unusable, unreadable or indecipherable to unauthorized individuals.

For purposes of the breach notification safe harbor, we do not believe that it is necessary to remove either the month or day of birth or the last three digits of a five digit zip code from data in LDS form. However, should HHS decide to require removal of this additional data for purposes of the Guidance, we request that the agency do so only on a prospective basis while providing a safe harbor for those LDSs created prior to the date of the final guidance. It likely will not be practical for covered entities to remove this data from an existing LDS. Entities should be able to take advantage of this safe harbor for an existing LDS. To do otherwise could create situations in which compliance with the breach notification requirements is impossible.

If HHS decides not to create a safe harbor for PHI in LDS form, AHA urges HHS to do so at least with respect to an LDS created before the final guidance. As noted above, many covered entities do not retain a key or code to re-identify patients whose health data are included in an

LDS made available under a Data Use Agreement. The LDS and Data Use Agreement is designed to protect patient privacy while permitting analyses that are critical for improving the safety, effectiveness and efficiency of our health care system. A failure to provide a safe harbor legacy LDS will create situations in which compliance with the breach notification requirements is impossible.

IV. Specification of Off-the-Shelf Products that Meet the Guidance's Encryption Standards

HHS has requested comments on whether future guidance should specify which off-the-shelf products, if any, meet the encryption standards set forth in the Guidance. The AHA does not believe that it would be beneficial for future guidance to specify which off-the-shelf products meet the encryption standards identified in the Guidance for a number of reasons. First, technological innovation proceeds too quickly for such a list to remain accurate. Reviewing new technologies for each annual update of the guidance could create an unnecessary burden for HHS. Second, a list would incentivize covered entities and business associates to standardize on the specifically approved products. This could stifle competition, resulting in higher prices for approved products and discouraging producers from pursuing new innovations. Third, industry standardization on a small number of products could increase the impact of security vulnerabilities identified in the approved products. Malicious programmers would be able to focus their attention on a limited universe of products. Once a vulnerability is identified in a product that is widely used, the covered entities and business associates who are using that product would be threatened. **To encourage innovation and minimize the impact of security vulnerabilities, the AHA urges HHS to refrain from specifying which off-the-shelf products meet its encryption standards.**

V. Comments on Breach Notification Provisions Generally

In recent years, many states have enacted data security laws that require individuals to be notified in the event of a breach of certain personally identifying information, and the AHA is pleased to provide additional comments below regarding covered entities' obligations under state breach notification laws to help inform the agency as it promulgates the interim final regulations on federal breach notification. HHS asked for comments in specific areas which we believe are related and, therefore, we address them jointly below.

Potential Areas of Conflict Between Federal and State Notice Obligations

While many of our member hospitals, health systems and networks operate within a single state and, therefore, are likely to maintain PHI primarily of residents of that state, it is easy to foresee circumstances where a hospital would maintain PHI of an individual who is a resident of a neighboring state or even a distant state, particularly where the hospital is known as a center of excellence in a particular field. In those circumstances, a hospital could be required to ensure that it is complying with multiple state, as well as federal, breach notice obligations.

While most of the state breach notification laws apply to breaches of personally identifying information other than health information, such as social security numbers (SSNs) or financial account numbers (e.g., credit cards), we believe that they are relevant to the extent that those types of identifiers are included in records with PHI maintained by hospitals. In the event of a breach of PHI, it is very likely that a hospital would have an obligation to provide notice under the applicable state, as well as the federal, law if in addition to health information some sensitive identifier such as an SSN was subject to the breach. Moreover, to the extent that CMS continues to use an individual's SSN as his or her Medicare number, it directly contributes to the problem for hospitals.

Risk of harm. One notable difference between the federal breach notification provision and most state provisions is the absence of a harm standard in the definition of breach. A majority of state breach notification laws provide that an incident is not a breach for which notice is required if there is no reasonable likelihood of harm (e.g., identity theft). **The AHA strongly urges HHS to adopt a similar "risk of harm" trigger for the federal breach notice requirement so that federal notice is not required when notice under state law is not required.**

The purpose of notifying individuals when their PHI has been the subject of a breach is to inform them to take certain precautions to mitigate harm. If a covered entity can conclude that there is no reasonable likelihood that harm would result to the affected individuals, no notice should be required. Our suggested harm standard is akin to the existing exception within HITECH's definition of breach (see section 13400 of Pub. L. No. 111-5, (Feb. 17, 2009)) for incidents "where an unauthorized person to whom [PHI] is disclosed would not reasonably have been able to retain such information."

Notifying individuals of an unauthorized acquisition, access or disclosure of their PHI should not be required when a covered entity, through investigation, has determined that there is no reasonable likelihood of harm to the individuals, serves no useful purpose. Instead, the federal notice would create unnecessary anxiety and concern among the individuals who would receive such notices and also would create an unnecessary and unproductive administrative burden and expense for the covered entity.

Consistency with respect to timing requirements. Another key area where there is conflict with the state breach notification requirements is the timing for providing notice to individuals. Most state laws do not require that notice be provided within a certain number of days. They simply require that notice be provided following discovery of the breach either "without unreasonable delay" or "in the most expedient time possible." In contrast, Section 13403(d)(1) requires the federal notice to affected individuals to be provided no later than 60 calendar days following the discovery of a breach.

The federal provision's inflexible timing requirement does not allow for unexpected but reasonable delays. For example, the investigation to determine the scope of the breach and identify the individuals affected may take longer than 60 days. If a covered entity is forced to send out notices before an investigation is complete, it may result in one of two problematic scenarios. First, there may be under-notification where the covered entity notifies the group of

individuals affected that certain data elements were compromised (e.g., procedure date and medical record number) by the 60-day deadline but then, upon further investigation, discovers that additional sensitive identifiers (e.g., SSN) also were compromised. The covered entity would be obligated to send out a follow-up notice, which would likely confuse and anger many of the recipients. The covered entity also would have to incur additional expense to send follow-up notices and address public relations issues that would likely arise if it appeared as though the covered entity did not conduct a thorough investigation. Alternatively, a covered entity may over-notify where it initially thinks the scope of the breach is larger than it really is and end up sending notices to more people than were actually affected. That scenario would result in unnecessary anxiety and confusion among those individuals who were notified improperly.

For these reasons, **we request clarifying guidance from HHS as to how to address reasonable delays due to investigation time and still comply with the 60-day requirement. In this regard, we suggest specifying that "discovery of the breach" means when a covered entity discovers that a single individual's PHI has been compromised, not when a covered entity discovers the breach incident (e.g., theft or hacking).** In practice, this would mean that the 60-day time period begins to run for notifying an individual at the time it is discovered that an individual's PHI was involved in the breach.

Circumstances Where the Required Federal Notice Would Not Also Satisfy Any Notice Obligations Under the State Law

If multiple states' notice requirements, as well as the federal notice requirement, apply to a single incident, it is possible that there will be situations in which the notice used for a specific breach incident cannot be standardized for all of the patients whose information may have been subject to the breach. If the content of the notice, for example, is required to reflect the law of the state where the patient resides, a hospital potentially would need to create multiple different notices in order to incorporate federal and applicable state requirements, particularly where state requirements are not compatible with one another or with the federal requirement. This would make breach notification even more costly and complex.

It is important to note that there is at least one state – Massachusetts – where compliance with the federal law would actually violate the state notice obligations. The Massachusetts security breach law, Mass. Gen. Law. chapter. 93H, section 3, requires that the notification "shall not include the nature of the breach or unauthorized acquisition or use" (emphasis added). In direct conflict, Section 13402(f) of the Act states that the federal breach notification must include a description of the breach.

While many of the state law conflicts arguably can be addressed by drafting a single communication that includes the required elements of both the federal and state law, the Massachusetts requirement to not disclose the nature of the breach cannot be similarly reconciled. Covered entities that maintain PHI of Massachusetts residents and experience a breach will not be able to comply with the required federal breach notice requirement without clearly violating the Massachusetts security breach notification law. Massachusetts is just one example. There is great uncertainty for covered entities trying to assess state security breach law obligations to

determine whether the state laws are preempted by the federal breach notice requirement or not which makes it an issue ripe for HHS interpretation.

Preemption

Because of the significant risk of confusion and incoherence in communicating with individuals about security breaches, we believe it is critical for HHS to include guidance clarifying the preemption provision at Section 13421(a) of the Act in the interim final regulation. We note that Section 13421(a) of the Act states that the preemption requirement set forth in the HIPAA statute (Section 1178 of the *Social Security Act*) that applies to the administrative simplification provisions also applies to the provisions of Subtitle D of the Act including the breach notification provision. Under the HIPAA administrative simplification and security preemption standard (42 U.S.C. § 1320d-7(a)(1) and (2)(B)), a federal provision preempts any contrary provision of state law, with certain specified exceptions such as if the state law relates to the privacy of individually identifiable health information. If the state law at issue relates to the privacy of individually identifiable health information, then the provision is not preempted unless it is contrary to a provision of the Privacy Regulation promulgated by HHS and is less stringent than the federal provision. See section 264(c)(2) of Pub. L. 104-191 and as a note to 42 U.S.C. § 1320d-2. Under the privacy HIPAA preemption standard, a federal regulation regarding the privacy of individually identifiable health information promulgated under section 264(c) does not preempt a contrary provision of state law if the state law requirement is more stringent and, therefore, more protective of patient health privacy than the federal regulation. This standard has proved to be extremely difficult in practice to apply to specific provisions of law.

Based on the plain language of Section 13421(a) of the Act, it is the administrative simplification HIPAA preemption standard that applies to the federal breach notification provisions. The AHA believes it is clear that because the statute takes this approach, the breach notification provisions should be regarded as relating to the security of individually identifiable health information, and not to privacy. Moreover, with three exceptions −Arkansas, California and Puerto Rico, which require notice for breaches of health or medical information − state breach notification laws apply generally to specific personal identifiers and not to individually identifiable ***health*** information.

Further, the AHA believes that in providing guidance regarding preemption, HHS should take notice of congressional intent to create a uniform and consistent breach notice requirement across state lines in the area of individually identifiable health information. To date, it has not done so with respect to other types of sensitive personal information where states already are heavily involved in promulgating laws. Such an approach would make it possible, for example, to apply the same legal standard when developing compliance procedures for integrating California law with federal law as the legal standard applied when integrating the requirements of Massachusetts law with federal law. It is extremely important to have a single, coherent preemption standard that consistently applies when covered entities are trying to integrate and coordinate state and federal breach notification requirements.

Therefore, we believe that it is imperative for HHS to provide preemption guidance with respect to its breach notification requirements in two areas. **First, HHS should conclude that state breach notification laws of general applicability do not "relate to the privacy of individually identifiable health information" for purposes of section 1178(a)(2)(B) of the *Social Security Act*, and thus are preempted by the federal breach notice standard when they are "contrary,"** as discussed further below. **Second, the AHA urges HHS to consider a more general provision establishing that breach notification provisions relate to the security of information and not to privacy, to better enable standardization of requirements even with respect to those few state laws that mention health information in their breach notification standards (as well as others that may choose to legislate in this area in the future).** We believe this is crucial to make it cost-effective to carry out the fundamental purposes of HITECH in building secure and workable electronic medical records systems that can be deployed in any state.

In addition, HHS should reiterate that, for purposes of the breach notification requirements, the term "contrary" is defined as being the definition promulgated for purposes of the Administrative Simplification, Security and Privacy provisions of HIPAA in 45 C.F.R. part 160. In other words, the term "contrary" should be construed to mean that either (1) a covered entity would find it impossible to comply with both the state and federal requirements, or (2) the provision of state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Subtitle D of the Act, specifically the breach notification provisions. See 45 C.F.R. section 160.202. In practice, such construction would mean that, if a covered entity could not comply with both federal and state breach notification requirements, then the state law requirement is contrary and preempted. Similarly, if a state law requirement frustrates the intent of the federal breach notice requirement, which is to create uniformity with respect to notifying individuals about breaches of PHI, then it is contrary and preempted. Following this reasoning, the Massachusetts requirement to not disclose the nature of the breach would be contrary to the federal requirement to provide a description of the breach and, therefore, should be preempted.

Statutory Breach Exceptions For Certain Internal Activities

HITECH provides certain exceptions to the definition of "breach," designed to limit the applicability of the breach notification requirements to covered entities' and business associates' internal operations. The AHA strongly believes that these breach exceptions must be implemented in a way that acknowledges the Privacy Rule and Security Rule's requirements for those entities. We believe that requiring breach notification requirements unnecessarily for internal uses and disclosures would not benefit patients but in fact could threaten their care. We request that HHS consider carefully its implementation of these breach exceptions, taking into account their potential effects on patient care delivery.

In particular, **we urge HHS to explain that the breach exception in Section 13400(1)(B)(i) of the statute applies only when there is no further unauthorized acquisition or disclosure of PHI.** This exception covers unintentional acquisition, access or use of PHI by an employee or individual acting under a covered entity or business associate's authority, when that acquisition,

access, or use was made in good faith and within the course of that employee or individual's employment or professional relationship with the covered entity or business associate and the PHI is not further acquired, accessed, used or disclosed by any person. **The AHA requests that HHS clarify that the breach notification requirements do not apply when any further acquisition, access, use or disclosure is authorized.** If HHS does not explain this element of the exception, a subsequent authorized disclosure would be considered a breach. This proposed exception is consistent with the other statutory exception; it also would help ensure efficient and effective application of the breach notification rule.

We believe it is imperative to avoid a situation in which the breach notification requirement applies to breaches within the workplace, which likely would be inadvertent and without a significant risk of harm. For that reason, **we strongly recommend that HHS adopt a risk of harm trigger for breach notification.** A risk of harm trigger would be consistent with the statutory language and would allow covered entities and business associates to avoid devoting considerable resources to notify affected individuals of an event that likely caused no harm.

The AHA strongly believes that the breach exceptions must be sufficiently broad to include routine internal uses or disclosures within a covered entity or business associate, or between a covered entity and a business associate. For example, we believe that the exceptions should reach circumstances in which a covered entity or business associate's employee or an individual acting on their authority transmits unsecured PHI to another covered entity or business associate, who handles it appropriately.

The AHA also requests that HHS apply the statute's second breach exception, set forth in Section 13400(B)(ii) and addressing inadvertent disclosures within a facility, in a manner that does not interfere with providers' ability to provide quality care**. If a health care entity has multiple locations and transmits information between those offices, each location should be considered part of the same facility for purposes of the breach exception so that the risk of technical breach notification violations does not interfere with the entity's health care activities.** As mentioned above, we strongly support a risk of harm standard for internal disclosures, and we believe such a standard is imperative to avoid devoting significant time and resources to notifying affected individuals of a "breach" that is harmless.

Obligation to Send Multiple Notices to an Individual Based on Discovery of a Single Breach

In the event that HHS does not construe the preemption provision at Section 13421(a) of the Act as suggested above, we strongly advise that HHS stipulate that the federal breach notice may include the required elements of the state breach notification laws to eliminate the need to send multiple notices to an individual based upon discovery of one breach.

Section 13402(f) of the Act specifies content requirements for the federal breach notice, including: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (2) a description of the types of unsecured PHI that were involved in the breach; (3) the steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity

involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number.

The state breach notification requirements for content of the notice are generally consistent with the state security breach laws. However, there are enough exceptions to necessitate having to send multiple notices to individuals of some states when there has been a single breach unless the state required elements can be combined with the federal required elements in one notice. Examples of some of the state-required elements include: contact information for all major national consumer reporting agencies under Iowa, Maryland, Oregon and Wyoming law; specific state government contact information (e.g., for the Office of the Attorney General) under Maryland law; advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports under Hawaii, Michigan, North Carolina, Vermont and Virginia law; and instructions to report suspected incidents of identity theft to law enforcement including the Federal Trade Commission under Iowa and Oregon law.

By clarifying that federal law permits combining state and federal notices, it will minimize anxiety and confusion among individuals who would otherwise receive two notice letters about the same incident and it would lessen the administrative burden of issuing two separate notice letters. The purpose of the notice is to alert the affected individual to take necessary precautions to prevent or mitigate potential harm or other effects of the breach. A single notice that includes the requirements of both federal and state law would still accomplish this purpose.

Circumstances Where State Law Obligates a Covered Entity to Notify Individuals Even When Information Has Been Rendered Secured Based on Federal Requirements

The federal requirements for securing PHI are encryption or destruction. If the PHI is secured by these means and a breach occurs, notice to the individual is not required. The AHA is not aware of circumstances where state law would obligate a covered entity to notify individuals of a breach where the information had been rendered secured based on federal requirements because the state notice requirements on this issue are similar. Depending on the state, notice of a breach is required under state law only where the breach involves personal information that was either not encrypted or not rendered unreadable or unusable by any other method or technology, or where it involves encrypted personal information and the confidential process or key to decrypt it. Despite this similarity between state and federal notice requirements, a need to notify affected individuals of a breach when information has been encrypted and thus secured based on the federal definition of encryption may arise if the state law defines encryption differently. **We urge HHS to clarify how covered entities should handle this situation or situations where the state law or regulation provides no definition of encryption.**