Own the Bone® and Data Use Agreements

Own the Bone® is a quality improvement program developed and managed by the American Orthopaedic Association (AOA). The AOA collects a "limited data set" as defined by HIPPA and therefore enters into Data Use Agreements with our participating sites.

AOA and Own the Bone do not enter into Business Associate Agreements for these two reasons:

1. The AOA Own the Bone Registry ("Registry") only collects only a "limited data set" as defined by HIPPA. According to guidance from the Department of Health and Human Services ("HHS") and a specific HIPAA regulation, if an entity collects only a Limited Data Set for the purpose of health care operations, the receiving entity and the covered entity sending the Limited Data Set are required to enter into a Data Use Agreement. The parties are not required to enter into a Business Associate Agreement.

2. The AOA includes within the Participating Site Agreement a fully compliant Data Use Agreement. Therefore, pursuant to the HIPAA regulation and guidance, AOA does not enter into Business Associate Agreements, but instead enters into Data Use Agreements.

Please refer to 45 CFR 164.504(e)(3)(iv), the HIPAA regulation, and the attached guidance from the HHS website. Please also refer to 45 CFR 164.514(e)(4) which sets forth the requirements for a Data Use Agreement.

If you have any questions about the program protocol and HIPAA data use provisions, please contact Stephanie Sofinski, Program Coordinator at sofinski@aoassn.org or at 847-318-7336.

indemnification clauses in business associate agreements.

Finally, several commenters requested that the Department provide a model business associate agreement.

Final Rule

The final rule adopts the proposed modifications to §§ 164.502(e) and 164.504(e). As we discussed above, while section 13404 of the HITECH Act provides that business associates are now directly liable for civil money penalties under the HIPAA Privacy Rule for impermissible uses and disclosures and for the additional HITECH requirements in Subtitle D that are made applicable to covered entities, it does not apply all of the requirements of the Privacy Rule to business associates and thus, the final rule does not. Therefore, business associates are not required to comply with other provisions of the Privacy Rule, such as providing a notice of privacy practices or designating a privacy official, unless the covered entity has chosen to delegate such a responsibility to the business associate, which would then make it a contractual requirement for which contractual liability would attach.

Concerning commenters' questions about the continued need for business associate agreements given the new direct liability on business associates for compliance, we note that section 13404 of the HITECH Act expressly refers and ties business associate liability to making uses and disclosures in accordance with the uses and disclosures laid out in such agreements, rather than liability for compliance with the Privacy Rule generally. Further, section 13408 of the HITECH Act requires certain data transmission and personal health record vendors to have in place business associate agreements with the covered entities they serve. We also continue to believe that, despite the business associate's direct liability for certain provisions of the HIPAA Rules, the business associate agreement is necessary to clarify and limit, as appropriate, the permissible uses and disclosures by the business associate, given the relationship between the parties and the activities or services being performed by the business associate. The business associate agreement is also necessary to ensure that the business associate is contractually required to perform certain activities for which direct liability does not attach (such as amending protected health information in accordance with § 164.526). In addition, the agreement represents an opportunity for the parties to clarify their respective responsibilities under the HIPAA Rules, such as by establishing how the business associate should handle a request for access to protected health information that it directly receives from an individual. Finally, the business associate agreement serves to notify the business associate of its status under the HIPAA Rules, so that it is fully aware of its obligations and potential liabilities.

With respect to questions about "satisfactory assurances," § 164.502(e) provides that covered entities and business associates must obtain and document the "satisfactory assurances" of a business associate through a written contract or other agreement, such as a memorandum of understanding, with the business associate that meets the applicable requirements of § 164.504(e). As discussed above, § 164.504(e) specifies the provisions required in the written agreement between covered entities and business associates, including a requirement that a business associate ensure that any subcontractors agree to the same restrictions and conditions that apply to the business associate by providing similar satisfactory assurances. Beyond the required elements at § 164.504(e), as with any contracting relationship, business associates and covered entities may include other provisions or requirements that dictate and describe their business relationship, and that are outside the governance of the Privacy and Security Rules. These may or may not include additional assurances of compliance or indemnification clauses or other risk-shifting provisions.

We also clarify with respect to the satisfactory assurances to be provided by subcontractors, that the agreement between a business associate and a business associate that is a subcontractor may not permit the subcontractor to use or disclose protected health information in a manner that would not be permissible if done by the business associate. For example, if a business associate agreement between a covered entity and a contractor does not permit the contractor to de-identify protected health information, then the business associate agreement between the contractor and a subcontractor (and the agreement between the subcontractor and another subcontractor) cannot permit the de-identification of protected health information. Such a use may be permissible if done by the covered entity, but is not permitted by the contractor or any subcontractors if it is not permitted by the covered entity's business associate agreement with the contractor. In short, each agreement in the business associate chain must be as stringent or more stringent as the agreement above with respect to the permissible uses and disclosures.

Finally, in response to the comments requesting a model business associate agreement, we note that the Department has published sample business associate provisions on its web site. The sample language is designed to help covered entities comply with the business associate agreement requirements of the Privacy and Security Rules. However, use of these sample provisions is not required for compliance with the Rules, and the language should be amended as appropriate to reflect actual business arrangements between the covered entity and the business associate (or a business associate and a subcontractor).

Response to Other Public Comments

Comment: Commenters requested guidance on whether a contract that complies with the requirements of the Graham Leach Bliley Act (GLBA) and incorporates the required elements of the HIPAA Rules may satisfy both sets of regulatory requirements. The commenters urged the Department to permit a single agreement rather than requiring business associates and business associate subcontractors to enter into separate GLBA agreements and business associate agreements.

Response: While meeting the requirements of the GLBA does not satisfy the requirements of the HIPAA Rules, covered entities may use one agreement to satisfy the requirements of both the GLBA and the HIPAA Rules.

Comment: A few commenters recommended adding an exception to having a business associate agreement for a person that receives a limited dataset and executes a data use agreement for research, health care operations, or public health purposes.

Response: We have prior guidance that clarifies that if only a limited dataset is released to a business associate for a health care operations purpose, then a data use agreement suffices and a business associate agreement is not necessary. To make this clear in the regulation itself, we are adding to § 164.504(e)(3) a new paragraph (iv) that recognizes that a data use agreement may qualify as a business associate's satisfactory assurance that it will appropriately safeguard the covered entity's protected health information when the protected health information disclosed for a health care operations purpose is a limited data set. A similar provision is not necessary or appropriate for disclosures of limited data sets for research or public health purposes since such disclosures would

not otherwise require business associate agreements.

Comment: A few commenters requested that the Department delete § 164.504(e)(2)(ii)(H), which provides that to the extent the business associate is to carry out a covered entity's obligation under the HIPAA Rules, the business associate must comply with the requirements of the HIPAA Rules that apply to the covered entity in the performance of the obligation on behalf of the covered entity. Alternatively, commenters suggested that the Department clarify that the requirements of the section need not be included in business associate agreements and that this section does not limit the ability of covered entities and business associates to negotiate responsibilities with regard to other sections of the Privacy Rule.

Response: The Department declines to delete § 164.504(e)(2)(ii)(H). If a business associate contracts to provide services to the covered entity with regard to fulfilling individual rights or other obligations of the covered entity under the Privacy Rule, then the business associate agreement must require the business associate to fulfill such obligation in accordance with the Privacy Rule's requirements. We do clarify, however, that if the covered entity does not delegate any of its responsibilities under the Privacy Rule to the business associate, then § 164.504(e)(2)(ii)(H) is not applicable and the parties are not required to include such language.

Comment: One commenter requested that the Department modify § 164.502(a)(4)(i) to permit business associates to use and disclose protected health information for their own health care operations purposes, and another commenter requested that the Department clarify whether § 164.504(e)(4) provides that a business associate may use or disclose protected health information as a covered entity would use or disclose the information.

Response: The Department declines to make the suggested modification. Business associates do not have their own health care operations (see the definition of health care operations at § 164.501, which is limited to activities of the covered entity). While a business associate does not have health care operations, it is permitted by § 164.504(e)(2)(i)(A) to use and disclose protected health information as necessary for its own management and administration if the business associate agreement permits such activities, or to carry out its legal responsibilities. Other than the exceptions for the business associate's management and administration and for data aggregation services relating to the health care operations of the covered entity, the business associate may not use or disclose protected health information in a manner that would not be permissible if done by the covered entity (even if such a use or disclosure is permitted by the business associate agreement).

Comment: One commenter suggested requiring subcontractors to return or destroy all protected health information received from or created for a business associate when the contract with the business associate is terminated.

Response: The final rule at § 164.504(e)(5) does apply the requirements at § 164.504(e)(2) through (4) (which set forth the requirements for agreements between covered entities and their business associates) to agreements between business associates and their subcontractors. This includes § 164.504(e)(2)(ii)(J), which requires the business associate to return or destroy all protected health information received from, or created or received on behalf of, the covered entity at the termination of the contract, if feasible. When this requirement is applied to the agreement between the business associate and its business associate subcontractor, the effect is a contractual obligation for the business associate subcontractor to similarly return or destroy protected health information at the termination of the contract, if feasible.

Comment: One commenter suggested requiring a business associate to disclose all subcontractors of the business associate to a covered entity within thirty days of the covered entity's request.

Response: The Department declines to adopt this suggestion as a requirement of the HIPAA Rules, because such a requirement would impose an undue disclosure burden on business associates. However, covered entities and business associates may include additional terms and conditions in their contracts beyond those required by § 164.504.

Comment: One commenter suggested establishing a certification process of business associates and subcontractors with regard to HIPAA compliance.

Response: The Department declines to establish or endorse a certification process for HIPAA compliance for business associates and subcontractors. Business associates and subcontractors are free to enlist the services of outside entities to assess their compliance with the HIPAA Rules and certification may be a useful compliance tool for entities, depending on the rigor of the program. However, certification does not guarantee compliance and therefore "certified" entities may still be subject to enforcement by OCR.

Comment: One commenter requested clarification on when it is not feasible for a business associate to terminate a contract with a subcontractor.

Response: Whether it is feasible for a business associate to terminate an agreement with a business associate subcontractor is a very fact-specific inquiry that must be examined on a case-by-case basis. For example, termination is not feasible for a business associate with regard to a subcontractor relationship where there are no other viable business alternatives for the business associate (when the subcontractor, for example, provides a unique service that is necessary for the business associate's operations). See our prior guidance on this issue as it applies to covered entities and business associates in Frequently Asked Question #236, available at *http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/236.html.*

c. Section 164.532—Transition Provisions

Proposed Rule

We understand that covered entities and business associates are concerned with the anticipated administrative burden and cost to implement the revised business associate agreement provisions of the Privacy and Security Rules. Covered entities may have existing contracts that are not set to terminate or expire until after the compliance date of the modifications to the Rules, and we understand that a six month compliance period may not provide enough time to reopen and renegotiate all contracts. In response to these concerns, we proposed to relieve some of the burden on covered entities and business associates in complying with the revised business associate provisions by adding a transition provision to grandfather certain existing contracts for a specified period of time. The Department's authority to add the transition provision is set forth in § 160.104(c), which allows the Secretary to establish the compliance date for any modified standard or implementation specification, taking into account the extent of the modification and the time needed to comply with the modification. The proposed transition period would prevent rushed and hasty changes to thousands of on-going existing business associate agreements. We addressed the issue of the business associate transition provisions as follows.

U.S. Department of Health & Human Services

Improving the health, safety, and well being of America

Health Information Privacy

If the only protected health information a business associate receives is a limited data set, does the HIPAA Privacy Rule require the covered entity to enter into both a business associate agreement and data use agreement with the business associate?

Answer:

No. Where a covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function, the covered entity satisfies the Rule's requirements that it obtain satisfactory assurances from its business associate with the data use agreement.

For example, where a State hospital association receives only limited data sets of protected health information from its member hospitals for the purposes of conducting and sharing comparative quality analyses with these hospitals, the member hospitals need only have data use agreements in place with the State hospital association.

Date Created: 12/19/2002
Last Updated: 03/14/2006

breach notification laws, as well as existing obligations on Federal agencies pursuant to OMB Memorandum M–07–16, that have similar standards for triggering breach notification. In addition, the standard was intended to ensure that consumers were not flooded with breach notifications for inconsequential events, which could cause unnecessary anxiety and eventual apathy among consumers.

To determine whether an impermissible use or disclosure of protected health information constitutes a breach under this standard, covered entities and business associates were required to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. In conducting the risk assessment, covered entities and business associates were to consider a number or combination of factors, including who impermissibly used the information or to whom the information was impermissibly disclosed; whether the covered entity or business associate had taken steps to mitigate or eliminate the risk of harm; whether the protected health information was actually accessed; and what type or amount of protected health information was impermissibly used or disclosed.

The rule provided further that an impermissible use or disclosure of protected health information that qualifies as a limited data set but also excludes dates of birth and zip codes (both identifiers that may otherwise be included in a limited data set) does not compromise the security or privacy of the protected health information. The Department included this narrow exception in the belief that it would be very difficult to re-identify a limited data set that excludes dates of birth and zip codes. Thus, a breach of such information would pose a low level of risk of harm to an individual.

The interim final rule also included the three statutory exceptions to the definition of breach. To implement section 13400(1)(B)(i) of the Act, the first regulatory exception provided that a breach excludes any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule. We substituted the term "workforce members" for the statutory term "employees" because "workforce member" is a defined term for purposes of the HIPAA Rules and means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate.

In addition to unintentional, good faith access to protected health information by workforce members, this exception covers similar access by a business associate of a covered entity or subcontractor with respect to a business associate or other person acting on behalf of a covered entity or business associate. The exception does not, however, cover situations involving snooping employees, because access as a result of such snooping would be neither unintentional nor done in good faith.

To implement section 13400(1)(B)(ii) and (iii) of the Act, the second regulatory exception provided that a breach excludes inadvertent disclosures of protected health information from a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates. The regulatory exception includes reference to an "organized health care arrangement" to capture, among other things, clinically integrated care settings in which individuals typically receive health care from more than one health care provider, such as a hospital, and the health care providers who have staff privileges at the hospital.

In this regulatory exception, we also interpreted the statutory limitations that the disclosure be to "another person similarly situated at the same facility" to mean that the disclosure be to another person authorized to access protected health information (even if the two persons may not be authorized to access the same types of protected health information) at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates (even if the covered entity, business associate, or organized health care arrangement has multiple facilities or locations across the country).

Finally, to implement section 13400(1)(A) of the Act, the interim final rule exempted disclosures of protected health information where a covered entity or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. For example, if a covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals and a few of the EOBs are returned by the post office, unopened, as undeliverable, the covered entity can conclude that the improper addressees could not reasonably have retained the information. The EOBs that were not returned as undeliverable, however, and that the covered entity knows were sent to the wrong individuals, should be treated as potential breaches. As another example, if a nurse mistakenly hands a patient the discharge papers belonging to another patient, but she quickly realizes her mistake and recovers the protected health information from the patient, this would not constitute a breach if the nurse can reasonably conclude that the patient could not have read or otherwise retained the information.

With respect to any of the three exceptions discussed above, a covered entity or business associate has the burden of proof, pursuant to § 164.414(b) (discussed below), for showing why breach notification was not required. Accordingly, the covered entity or business associate must document why the impermissible use or disclosure falls under one of the above exceptions.

Overview of Public Comments

Of the approximately 85 public comments received on the interim final rule addressing the definition of breach, approximately 70 of those comments addressed the harm standard and risk assessment approach in the interim final rule. We received approximately 60 comments in support of the harm standard and the risk assessment approach. The commenters in support of this approach included providers, health plans, professional associations, and certain members of Congress. These commenters argued that the inclusion of the harm standard and accompanying risk assessment was consistent with the statutory language, aligned the interim final rule with many State breach notification laws and Federal policies, and appropriately placed the obligation to determine if a breach had occurred on covered entities and business associates since they had the requisite knowledge of the incident to best assess the likely impact of the impermissible use or disclosure.

The proponents of the harm standard and risk assessment approach also argued that its removal would increase the cost and burden of implementing the rule for covered entities, business associates, as well as HHS, and may cause unnecessary anxiety and eventual

In addition to the removal of the harm standard and the creation of more objective factors to evaluate the probability that protected health information has been compromised, we have removed the exception for limited data sets that do not contain any dates of birth and zip codes. In the final rule, following the impermissible use or disclosure of any limited data set, a covered entity or business associate must perform a risk assessment that evaluates the factors discussed above to determine if breach notification is not required.

The vast majority of commenters were not supportive of the exception for certain limited data sets outlined in the interim final rule, either because they believed the exception did not go far enough and would chill research that needed access to birth dates and zip codes in limited data sets, or because of concerns regarding the re-identifiability of the limited information to which the exception applied. Based on the comments, we believe it is appropriate to require the impermissible use or disclosure of a limited data set, even those that do not contain dates of birth and zip codes, to be subject to a risk assessment to demonstrate that breach notification is not required. The final rule expressly includes a factor that would require consideration of the re-identifiability of the information, as well a factor that requires an assessment of the unauthorized person who used the protected health information or to whom the disclosure was made (i.e., whether this person has the ability to re-identify the affected individuals). Thus, the factors are particularly suited to address the probability that a data set without direct identifiers has been compromised following an impermissible use or disclosure. Further, we believe in most cases that the result would be the same under this final rule as under the interim final rule with respect to whether an impermissible use or disclosure of a limited data set that also excludes dates of birth and zip codes constitutes a breach for which notification is required. Due to the lack of identifiers present in the protected health information, entities may reasonably determine that there is a low probability of risk that the information has been compromised; however, we stress that this is a fact specific determination to be made based on the circumstances of the impermissible use or disclosure.

We encourage covered entities and business associates to take advantage of the safe harbor provision of the breach notification rule by encrypting limited data sets and other protected health information pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740, 42742). If protected health information is encrypted pursuant to this guidance, then no breach notification is required following an impermissible use or disclosure of the information.

In addition to the comments discussed above, it was suggested that covered entities be required to include in their notice of privacy practices information about how a risk assessment will be conducted or their internal policies for determining whether a breach has occurred and notification is warranted. It was also suggested that the breach notice to the individual following discovery of a breach of unsecured protected health information contain information about the covered entity or business associate's risk assessment to help the individual better assess the level of threat posed by the breach and to better determine the appropriate steps, if any, to take.

We decline to require that the covered entity's notice of privacy practices include a description of how a risk assessment will be conducted, although covered entities may include such information in their notice of privacy practices if they choose. While each risk assessment will differ depending on the specific facts and circumstances surrounding the impermissible use or disclosure, we believe that the modifications in this final rule will help ensure that covered entities and business associates perform risk assessments more uniformly and objectively. We also note that the content requirements for the notice to the individual outlined in § 164.404(c) already require that the individual be notified of the circumstances of a breach, as well as what steps individuals should take to protect themselves from potential harm resulting from the breach.

One commenter suggested that we require a covered entity to hire an independent organization to assess the risk of an impermissible use or disclosure to determine if breach notification is required. We do not believe such a requirement is necessary, although covered entities are free to engage independent organizations to assist in making such determinations provided that, if access to protected health information is required, business associate agreements are entered into to protect the information. Further, we believe the modifications in this final rule are conducive to more uniform risk assessments across covered entities and business associates. Additionally, as with the interim final rule, we note that covered entities and business associates have the burden of proof, pursuant to § 164.414, to demonstrate that all notifications were provided or that an impermissible use or disclosure did not constitute a breach and to maintain documentation (e.g., of the risk assessment demonstrating that there was a low probability that the protected health information had been compromised or of the assessment that the impermissible use or disclosure falls within one of the other exceptions to breach), pursuant to 45 CFR 164.530(j)(1)(iv), as necessary to meet this burden of proof. Thus, covered entities and business associates have adequate incentive to conduct reasonable and diligent risk assessments.

Finally, after reviewing and considering the comments received regarding the exceptions to the definition of breach in the interim final rule, the Department adopts these exceptions without modification in this final rule. Although the substance of these exceptions has not changed, these exceptions are now located at paragraph (1) of the definition of breach instead of paragraph (2) to accommodate the modifications discussed above. We respond to the public comments addressing these exceptions, as well as other comments received on the definition of "breach," below.

Response to Other Public Comments

Comment: Many commenters expressed concern that violations of the minimum necessary standard may trigger breach notification obligations.

Response: We do not believe it would be appropriate to exempt minimum necessary violations from the breach notification obligations as we do not believe that all minimum necessary violations present a low probability that the protected health information has been compromised. Thus, uses or disclosures that impermissibly involve more than the minimum necessary information, in violation of §§ 164.502(b) and 164.514(d), may qualify as breaches. Such incidents must be evaluated as any other impermissible uses or disclosures to determine whether breach notification is not required.

As explained above, there are several factors to be considered when determining the probability that the protected health information involved in an impermissible use or disclosure has been compromised, including the