Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Business Associates' Use of Information for Their Own Purposes

Insight — September 6, 2019

Business associates may want to use a covered entity's protected health information ("PHI") for the business associates' own purposes, *e.g.*, for their own product development, data aggregation, marketing, *etc.* However, with very limited exceptions, HIPAA prohibits business associates from doing so without the patient's written authorization. Misusing PHI may expose the business associate to HIPAA fines, criminal penalties, breach of contract claims by the covered entity, and perhaps civil liability to individuals whose PHI was improperly used. (*See*, *e.g.*, 42 U.S.C. § 1320d-6; 45 C.F.R. § 160.404).

Limits on Use or Disclosure of PHI.

The business associate's authority to use or disclose PHI derives from the covered entity's authority. The covered entity may only use the patient's PHI for certain purposes without the patient's authorization, *e.g.*, for the covered entity's own treatment, payment or healthcare operations. (45 C.F.R. § 164.502). HIPAA allows covered entities to share PHI with business associates to assist the covered entity in performing authorized activities for or on behalf of the covered entity, but with very limited exceptions, the same limits that apply to the covered entity also apply to the business associate, *e.g.*, absent the patient's written authorization, it may only use the information for purposes of the covered entity's treatment, payment, healthcare operations or other permitted use. (*Id.*). The business associate agreement ("BAA") between the covered entity and business associate must specify the permissible uses of PHI. 45 C.F.R. § 164.502(e) states:

> (2) *Implementation specifications: Business associate contracts*. A contract between the covered entity and a business associate must:
>
> > (i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of [the HIPAA privacy rule] if done by the covered entity, except that:
> >
> > > (A) *The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate*, as provided in paragraph (e)(4) of this section; and
> >
> > > (B) *The contract may permit the business associate to provide*

> *data aggregation services relating to the health care operations of the covered entity.*
>
> (ii) Provide that the business associate will:
>
> (A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;
>
> …
>
> (4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary:
>
> (A) For the proper management and administration of the business associate; …

(Emphasis added). Thus, HIPAA identifies two exceptions in which the business associate may use PHI for its own purposes without the patient's authorization: (1) to perform data aggregation services, and (2) for the business associate's own management and administration. (65 F.R. 82505-06).

The Data Aggregation Exception.

> *Data aggregation* means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that *relate to the health care operations of the respective covered entities*.

(45 C.F.R. § 164.501, emphasis added). Per the regulation, the business associate may only aggregate the PHI for the healthcare operations of the covered entity, not for the business associate's own purposes. HHS commentary explains the purpose and scope of the exception:

> we permit a covered entity to authorize the business associate to provide data aggregation services *to the covered entity*. As discussed above in § 164.501, data aggregation, with respect to protected health information received by a business associate in its capacity as the business associate of a covered entity, is the combining of such protected health information by the business associate with protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit the creation of data for analyses that *relate to the health care operations of the respective covered entities*. We added this service to the business associate definition to clarify the ability of covered entities to contract

> with business associates to undertake quality assurance and comparative analyses that involve the protected health information of more than one contracting covered entity. We except data aggregation from the general requirement that a business associate contract may not authorize a business associate to use or further disclose protected health information in a manner that would violate the requirements of this subpart if done by the covered entity in order to permit the combining or aggregation of protected health information received in its capacity as a business associate of different covered entities when it is performing this service. In many cases, the combining of this information *for the respective health care operations of the covered entities* is not something that the covered entities could do—a covered entity cannot generally disclose protected health information to another covered entity for the disclosing covered entity's health care operations. However, we permit covered entities that enter into business associate contracts with a business associate for data aggregation to permit the business associate to combine or aggregate the protected health information they disclose to the business associate *for their respective health care operations*.

(65 F.R. 82505-06, emphasis added). Per the regulations and commentary, the "data aggregation" exception would not apply unless (1) the data aggregation is for the covered entity's healthcare operations, not the business associate's own purposes; and (2) the BAA expressly authorizes the business associate to perform the data aggregation services.

The Management and Administration Exception. HHS has not defined "management and administration," nor has it clearly delineated the boundaries of the exception applicable to business associates. The Privacy Rule does allow covered entities to use PHI for their "health care operations", which is defined to include:

> *Business management and general administrative activities of the entity*, including, but not limited to:
> (i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
> (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
> (iii) Resolution of internal grievances;
> (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
> (v) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

(45 C.F.R. § 164.501, definition of *health care operations*, emphasis added). HHS's use of similar terms (*i.e.*, the covered entity's "business management and general administrative activities" compared to the

business associate's “management and administration”) arguably suggests that the business associate may use PHI for similar internal operations. However, the limited commentary we have received suggests that “management and administration” should be construed relatively narrowly. For example, The OCR has explained:

> Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

(OCR Guidance at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf). In the health information organization (“HIO”) context, the OCR published the following FAQ:

> *What may a HIPAA covered entity's business associate agreement authorize a health information organization (HIO) to do with electronic protected health information (PHI) it maintains or has access to in the network?*
>
> A business associate agreement may authorize a business associate to make uses and disclosures of PHI the covered entity itself is permitted by the HIPAA Privacy Rule to make. *See* 45 C.F.R. § 164.504(e). In addition, the Privacy Rule permits a business associate agreement to authorize a business associate (*e.g.*, a HIO) to: (1) use and disclose PHI for the proper management and administration of the business associate, in accordance with 45 C.F.R. § 164.504(e)(4); and (2) to provide data aggregation services related to the health care operations of the covered entities for which it has agreements. In most cases, the permitted uses and disclosures established by a business associate agreement will vary based on the particular functions or services the business associate is to provide the covered entity. Similarly, a covered entity's business associate agreement with a HIO will vary depending on a number of factors, such as the electronic health information exchange purpose which the HIO is to manage, the particular functions or services the HIO is to perform for the covered entity, and any other legal obligations a HIO may have with respect to the PHI. For example, the business associate agreements between covered entities and a HIO may authorize the HIO to:
>
> - Manage authorized requests for, and disclosures of, PHI among participants in the network;
> - Create and maintain a master patient index;
> - Provide a record locater or patient matching service;
> - Standardize data formats;
> - Implement business rules to assist in the automation of data exchange;
> - Facilitate the identification and correction of errors in health information records; and

- Aggregate data on behalf of multiple covered entities.

(https://www.hhs.gov/hipaa/for-professionals/faq/543/what-may-a-covered-entitys-business-associate-agreement-authorize/index.html). Note that the permitted uses relate closely to the services the business associate performs for the covered entities.

HHS has confirmed that the "management and administration" exception does *not* extend to data mining for the business associate's own purposes:

> *Comment:* A commenter recommended that the business partner contract specifically address the issue of data mining because of its increasing prevalence within and outside the health care industry.
>
> *Response:* We agree that protected health information should only be used by business associates for the purposes identified in the business associate contract. We address the issue of data mining by requiring that the business associate contract explicitly identify the uses or disclosures that the business associate is permitted to make with the protected health information. Aside from disclosures for data aggregation and business associate management, the business associate contract cannot authorize any uses or disclosures that the covered entity itself cannot make. Therefore, data mining by the business associate for any purpose not specified in the contract is a violation of the contract and grounds for termination of the contract by the covered entity.

(65 F.R. 82644). Similarly, OCR FAQs confirm that a business associate may not use PHI for its own marketing purposes:

> *Can contractors (business associates) use protected health information for its own marketing purposes?*
>
> *Answer:* No. While covered entities may share protected health information with their contractors who meet the definition of "business associates" under the HIPAA Privacy Rule, that definition is limited to contractors that obtain protected health information to perform or assist in the performance of certain health care operations on behalf of covered entities. Thus, business associates, with limited exceptions, cannot use protected health information for their own purposes…. [T]he Privacy Rule expressly prohibits … covered health care providers from selling protected health information to third parties for the third party's own marketing activities, without authorization. So, for example, a pharmacist cannot, without patient authorization, sell a list of patients to a pharmaceutical company, for the pharmaceutical company to market its own products to the individuals on the list.

(https://www.hhs.gov/hipaa/for-professionals/faq/276/can-business-associates-use-protected-health-information-for-marketing/index.html).

I found no HHS or OCR commentary authorizing a business associate to use PHI for its own product development purposes under the "management and administration" function. Absent such commentary, I think a business associate's use of PHI for its own product development

purposes is risky unless such product development is within the scope of the services performed by the business associate for the covered entity as specified in the BAA.

De-Identification. Although HIPAA limits the business associate's use of PHI for its own purposes, the BAA may authorize the business associate to de-identify PHI on behalf of the covered entity client. (*See* 45 C.F.R. § 164.502(d)). Once de-identified, the information is no longer protected by HIPAA and, unless otherwise limited by the agreements between the parties or other law, the business associate may use the de-identified information for its own purposes without violating HIPAA. The OCR published the following FAQ addressing this issue:

> *May a health information organization (HIO), acting as a business associate of a HIPAA covered entity, de-identify information and then use it for its own purposes?*
>
> A HIO, as a business associate, may only use or disclose protected health information (PHI) as authorized by its business associate agreement with the covered entity. *See* 45 C.F.R. § 164.504(e). The process of de-identifying PHI constitutes a use of PHI. Thus, a HIO may only de-identify PHI it has on behalf of a covered entity to the extent that the business associate agreement authorizes the HIO to do so. However, once PHI is de-identified in accordance with the HIPAA Privacy Rule, it is no longer PHI and, thus, may be used and disclosed by the covered entity or HIO for any purpose (subject to any other applicable laws).

(https://www.hhs.gov/hipaa/for-professionals/faq/544/may-a-health-information-organization-de-identify-information/index.html).

Conclusion. PHI in the hands of the business associate is still protected. The general rule remains that a business associate may not use the PHI for its own purposes without the patient's authorization. To use PHI for its own purposes, the business associate should ensure that the BAA authorizes the use, HIPAA permits the business associate to use the PHI to perform a function on behalf of the covered entity or the use fits within the relatively limited “management and administration” exception, or the business associate secures the authorization of the patient.

For questions regarding this update, please contact:
Kim C. Stanger
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
email: kcstanger@hollandhart.com, phone: 208-383-3913

Substantive changes in the law subsequent to the date of this publication might affect the analysis or commentary. Similarly, the analysis may differ depending on the jurisdiction or circumstances. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.

Subscribe to get our Insights delivered to your inbox.