DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services 7500
Security Boulevard, Mail Stop N1-19-21Baltimore,
Maryland 21244-1850

Administrative Simplification

Go to Guidance
BRINGING YOU CLARITY AND TRANSPARENCY

Date: March 22, 2022 GL-2022-03

Subject: **Guidance on HIPAA Covered Entities' responsibility to require that Business Associates' comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations.**

The Department of Health and Human Services (HHS) is issuing this guidance to clarify covered entities' obligation to require that business associates comply with HIPAA regulations, as specified by 45 Code of Federal Regulations (C.F.R.) § 162.923(c).

Issues: The Office of Burden Reduction and Health Informatics' (OBRHI) National Standards Group (NSG) frequently receives, on behalf of HHS, complaints alleging noncompliance with HIPAA Administrative Simplification requirements filed against entities conducting HIPAA standard transactions that do not meet the regulatory definition of a "covered entity." Such entities typically function as business associates to HIPAA covered entities, and provide services to, or conduct transactions on behalf of, covered entities. The complaints frequently allege noncompliance with standards for electronic health care transactions, code sets, unique identifiers, and operating rules. These scenarios raise two principal questions:

1. **Must a covered entity's business associate comply with HIPAA Administrative Simplification requirements related to standards for electronic transactions, code sets, unique identifiers, and operating rules?**
2. **If HHS finds that a covered entity's business associate has violated, or is in violation of, an applicable Administrative Simplification requirement, is a covered entity responsible for its business associate's noncompliance?**

Key Regulatory Provisions:

A covered entity is defined at 45 C.F.R. § 160.103 as a health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction for which a standard has been adopted.

Under 45 C.F.R. § 162.923(c), covered entities -

> may use a business associate, including a health care clearinghouse, to conduct a transaction covered by this part. If a covered entity chooses to use a business associate to conduct all or part of a transaction on behalf of the covered entity, the covered entity must require the business associate to do the following:
>
> (1) Comply with all applicable requirements of this part.
>
> (2) Require any agent or subcontractor to comply with all applicable requirements of this part.

A business associate is defined at 45 C.F.R. § 160.103 and generally includes any person, including a partnership, corporation, or other public or private entity, that performs functions or activities related to electronic transactions for

which the Secretary has adopted a standard under HIPAA or provides certain other listed services to a covered entity. Members of a covered entity's workforce are not business associates.

Analysis:

1. **Must a covered entity's business associate comply with HIPAA Administrative Simplification requirements related to standards for electronic transactions, code sets, unique identifiers, and operating rules?**

Business associates are indirectly required to comply with HIPAA Administrative Simplification requirements.

Requirements related to standards for electronic transactions, code sets, unique identifiers, and operating rules apply only to covered entities, but 45 C.F.R. § 162.923(c) requires covered entities to require their business associates to comply. Effectively, this means that when a covered entity engages a business associate to conduct all or part of a transaction for which a standard has been adopted on behalf of the covered entity, the business associate, and any agents or subcontractors thereof, must comply with applicable requirements.

2. **If HHS finds that a covered entity's business associate has violated, or is in violation of, an applicable Administrative Simplification requirement, is a covered entity responsible for its business associate's noncompliance?**

Yes. A covered entity is responsible for the noncompliance of its business associate where the business associate does not comply with an applicable HIPAA Administrative Simplification requirement.

Engaging a business associate to provide services related to a transaction for which a standard has been adopted does not relieve a covered entity from its responsibility to comply with all applicable requirements. When providing services related to a transaction for which a standard has been adopted, a business associate is acting on behalf of a covered entity, and the business associate's actions or inactions are imputed to the covered entity. NSG may find a covered entity noncompliant if its business associate's action or inaction is noncompliant with an applicable HIPAA Administrative Simplification requirement.

For example, a health plan may engage a business associate to transmit remittance advices to health care providers on behalf of the health plan. Should a business associate send electronic transactions containing remittance advices that do not use the adopted standard at 45 C.F.R. § 162.1602(d)(2), the ***health plan*** may be found noncompliant with 45 C.F.R. § 162.923(a) for failure to conduct a transaction using the adopted standards. NSG may also find the health plan noncompliant with 45 C.F.R. § 162.923(c) for failure to require the business associate to comply with the applicable standard. A business associate's actual noncompliance could be used as evidence of a covered entity's failure to require its business associate to comply with all applicable requirements, irrespective of whether an agreement between a covered entity and a business associate obligates the business associate to comply with all applicable requirements.

Should NSG find that a covered entity is noncompliant due to its business associate's actions or inactions, NSG's

recourse to address the noncompliance would be against the covered entity.[1] This includes holding the covered entity responsible for satisfying any plan of corrective action and for payment of any civil money penalty.

Of note, health plans, health care clearinghouses, and health care providers that meet the definition of a covered entity may serve as business associates to other covered entities. Regardless of whether a business associate is itself a covered entity, when serving in a business associate capacity for a covered entity that is a party to a transaction, the covered entity that is party to the transaction can be held accountable for the business associate's noncompliance. For example, a health care provider may have an arrangement with a vendor to process health information for a health care claim from the provider into the standard format to transmit to a health plan. Section 45 C.F.R. § 162.1101(a) defines a health care claims transaction to include "[a] request to obtain payment, and the necessary accompanying information ***from a health care provider to a health plan*** for health care" (emphasis added). In this situation, the provider is the party to the health care claims transaction and the vendor is acting as the provider's business associate. Although the vendor meets the definition of a health care clearinghouse, and therefore is a covered entity in its own right, the provider could be held responsible for the vendor's noncompliant actions or inactions while acting on the provider's behalf.

Additional Information

Should you have questions about this guidance, send inquiries to AdministrativeSimplification@cms.hhs.gov with the subject line: Business Associate Guidance Question. Questions on other topics related to the adopted standards or operating rules may be sent to this same e-mail address. For more information, visit the CMS Administrative Simplification website at go.cms.gov/AdminSimp. For the latest news about Administrative Simplification, sign up for Email Updates at https://public.govdelivery.com/accounts/USCMS/subscriber/new?topic_id=USCMS_7834.

Sincerely,

Christine Gerhardt -S Digitally signed by Christine Gerhardt -S
Date: 2022.03.21 12:15:46 -04'00'

Christine Gerhardt
Director, National Standards Group

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law, regulations, or agency policy. This document was produced and disseminated at U.S. taxpayer expense. The funds used to produce this document were derived from amounts made available to the agency for advertising or other communications regarding the programs and activities of the agency.

[1] Consistent with the HITECH Act (enacted as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. 111-5), the HHS Office for Civil Rights (OCR) issued a final rule in 2013 to modify the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, (78 FR 5566, January 25, 2013), establishing that HHS has the authority to take enforcement action directly against business associates only for specific provisions of the HIPAA Security and Privacy Rules. The HITECH Act did not extend direct liability to business associates for Administrative Simplification provisions related to standards for transactions, code sets, unique identifiers, or operating rules. OCR Published a fact sheet on Direct Liability of Business Associates at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html