New HHS Fact Sheet on
Direct Liability of Business Associates under HIPAA

May 24, 2019

In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act,[1] making business associates of covered entities directly liable for compliance with certain requirements of the HIPAA Rules. Consistent with the HITECH Act, the HHS Office for Civil Rights (OCR) issued a final rule in 2013 to modify the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules.[2] Among other things, the final rule identifies provisions of the HIPAA Rules that apply directly to business associates and for which business associates are directly liable.[3]

As set forth in the HITECH Act and OCR's 2013 final rule, OCR has authority to take enforcement action against business associates only for those requirements and prohibitions of the HIPAA Rules as set forth below.

Business associates are directly liable for HIPAA violations as follows:

1. Failure to provide the Secretary with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the Secretary to information, including protected health information (PHI), pertinent to determining compliance.[4]

2. Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in an investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA Rules.[5]

3. Failure to comply with the requirements of the Security Rule.[6]

4. Failure to provide breach notification to a covered entity or another business associate.[7]

5. Impermissible uses and disclosures of PHI.[8]

6. Failure to disclose a copy of electronic PHI (ePHI) to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement) to satisfy a covered entity's obligations regarding the form and format, and the time and manner of access under 45 C.F.R. §§ 164.524(c)(2)(ii) and 3(ii), respectively.[9]

7. Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.[10]

8. Failure, in certain circumstances, to provide an accounting of disclosures.[11]

9. Failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for such agreements.[12]

10. Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement.[13]

For example, where the business associate's agreement with a covered entity requires it to provide an individual with an electronic copy of his or her ePHI upon the individual's request and the business associate fails to do so, OCR has enforcement authority directly over the business associate for that failure. (*See* No. 6 above.)

By contrast, OCR lacks the authority to enforce the "reasonable, cost-based fee" limitation in 45 C.F.R. § 164.524(c)(4) against business associates because the HITECH Act does not apply the fee limitation provision to business associates. A covered entity that engages the services of a business associate to fulfill an individual's request for access to their PHI is responsible for ensuring that, where applicable, no more than the reasonable,

cost-based fee permitted under HIPAA is charged. If the fee charged is in excess of the fee limitation, OCR can take enforcement action against only the covered entity.

Footnotes

- 1. The HITECH Act was 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.
- 2. 78 FR 5566 (January 25, 2013).
- 3. See 78 FR 5566.
- 4. See 45 CFR §§ 160.310, 164.502(a)(4)(i).
- 5. See 45 CFR § 160.316.
- 6. See HITECH Act § 13401, 42 USC § 17931 (making 45 CFR §§ 164.308, 164.310, 164.312, and 164.316 directly applicable to business associates, as well as any other security provision that the HITECH Act made applicable to covered entities); 45 CFR §§ 164.306, 164.308, 164.310, 164.312, 164.314, 164.316.
- 7. See 45 CFR §§ 164.410, 164.412.
- 8. See 45 CFR § 164.502(a)(3).
- 9. See 45 CFR § 164.502(a)(4)(ii).
- 10. See 45 CFR § 164.502(b).
- 11. See HITECH Act § 13405(c)(3), 42 U.S.C. § 17935(c)(3) (“A business associate included on a list under subparagraph (b) shall provide an accounting of disclosures (as required under paragraph (1) for a covered entity) made by the business associate upon a request made by an individual directly to the business associate for such an accounting.”). OCR plans to issue rulemaking on the accounting of disclosures as required by HITECH Act § 13405(c)(2).
- 12. See 45 CFR §§ 164.502(e)(1)(ii), 164.504(e)(5).
- 13. See 45 C.F.R. § 164.504(e)(1)(iii) (“A business associate is not in compliance with the standards in §164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.”).

HIPAA Security Rule

Administrative Safeguards			
Standards	**CFR Sections**	**Implementation Specifications (R)=Required (A)=Addressable**	
Security Management Process	164.308(a)(1)	**Risk Analysis**	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)	**none**	(R)
Workforce Security	164.308(a)(3)	**Authorization and/or Supervision**	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	**Isolating Healthcare Clearinghouse Function**	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	**Security Reminders**	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	**Response and Reporting**	(R)
Contingency Plan	164.308(a)(7)	**Data Backup Plan**	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)	**none**	(R)
Business Associate Contracts	164.308(b)(1)	**Written Contract or Other Arrangement**	(R)
Physical Safeguards			
Standards	**CFR Sections**	**Implementation Specifications (R)=Required (A)=Addressable**	
Facility Access Controls	164.310(a)(1)	**Contingency Operations**	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)	**none**	(R)
Workstation Security	164.310(c)	**none**	(R)
Device and Media Controls	164.310(d)(1)	**Media Disposal**	(R)
		Media Re-use	(R)
		Media Accountability	(A)
		Data Backup and Storage (during transfer)	(A)
Technical Safeguards			
Standards	**CFR Sections**	**Implementation Specifications (R)=Required (A)=Addressable**	
Access Control	164.312(a)(1)	**Unique User Identification**	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption (data at rest)	(A)
Audit Controls	164.312(b)	**none**	(R)
Integrity	164.312(c)(1)	**Protection Against Improper Alteration or Destruction of Data**	(A)
Person or Entity Authentication	164.312(d)	**none**	(R)
Transmission Security	164.312(e)(1)	**Integrity Controls**	(A)
		Encryption (FTP and Email over Internet)	(A)

Required vs. Addressable

HIPAA Implementation Specifications are identified as being *Required or Addressable. Addressable* specifications are sometimes confused as being Optional, which is not true. The US Department of Health & Human Services says ***"a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative."*** *If you believe that an Addressable specification is not reasonable or appropriate, you must* document your decision.