
Rules for Business Associate Agreements Need Clarification

December 15, 2011

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts [here](#):

- [1\) CDT Supports Expansion of HIPAA to Cover Business Associates and their Subcontractors](#)
- [2\) Current and Proposed Rules Regarding Business Associate Agreements Needs Clarification](#)
- [3\) Correct Implementation of Expanded Scope is Key](#)
- [4\) Privacy and Security Tiger Team Recommendations](#)

Summary

A comprehensive framework of privacy and security protections for personal health data, based on Fair Information Practices (FIPs), is crucial to building and maintaining consumer trust in health information technology (health IT) and health information exchange. The privacy provisions in the HITECH portion of the American Recovery and Reinvestment Act of 2009 took significant steps toward establishing this comprehensive framework, as did the July 2010 notice of proposed rulemaking (NPRM) implementing them. CDT submitted comments to this rule in September of 2010, stating that we were encouraged that many of the provisions in the NPRM would further fortify patient privacy, data security and enforcement of the law.

However, we remain concerned that the HIPAA Privacy Rule is still not sufficiently clear with respect to the access, use and disclosure of health information by "business associates," entities that received personal health information in order to perform a service or function on behalf of a HIPAA covered entity like a health care provider or health plan. Consistent with FIPs, a business associate's ability to access and disclose personal health information should be limited to what is reasonably necessary for them to fulfill their responsibilities to the covered entity. Ideally, these limits on how a business associate can access and disclose personal health information should be part of the contract or business associate agreement (BAA) between the parties. But the HIPAA Privacy Rule today does not unambiguously require BAAs to place clear limits on how business associates and their subcontractors can use and disclose patient data received from covered entities.

CDT recently testified on the business associate provisions in the current HIPAA Privacy Rule before the Senate Judiciary Subcommittee on Privacy, Technology and the Law. This Policy Post provides a more detailed analysis of the concerns raised in that testimony.

[Summary of Health Privacy Provisions in ARRA](#) [1]

[CDT Comments to HHS Proposed Rulemaking](#) [2]

[Deven McGraw Testimony](#) [3]

1) CDT Supports Expansion of HIPAA to Cover Business Associates and their Subcontractors

CDT was pleased with the provisions in HITECH extending accountability for violations of HIPAA to business associates. Previously, regulators had very limited authority over business associates. Providing regulators with the authority to enforce the HIPAA regulations against business associates is a positive development and brings the nation a step closer to achieving comprehensive protections for health data regardless of what entity is accessing, using or disclosing it.

We also strongly supported the clarification in the NPRM that the accountability of business

associates under HITECH extends to subcontractors of business associates, which is a positive step toward maintaining a more consistent level of accountability for privacy protection as personal health data moves downstream. Any break in the chain of public accountability once information is disclosed breaches the public's trust and is an obstacle to encouraging greater information flows to improve individual and population health.

2) Current and Proposed Rules Regarding Business Associate Agreements Needs Clarification

CDT was pleased to see the NPRM restate a number of strong Privacy Rule provisions that indicate a BAA should be a tool for limiting a business associate's use and disclosure of PHI received from a covered entity, such as:

- Proposed section 164.504(e)(2) states that BAAs must “establish the permitted and required uses and disclosures of protected health information (PHI) by the business associate... [and] may not authorize the business associate to use or further disclose the information in a manner” that would violate HIPAA.
- The BAA also must bind the business associate to not using or disclosing information other than as permitted or required by the contract or as required by law.

Unfortunately, the NPRM also retains other BAA provisions from the Privacy Rule that have been viewed by consumer and privacy advocates as providing business associates with too much discretion with respect to uses and disclosures of PHI. For example:

- Business associates are still permitted to use and disclose PHI for the "proper management and administration of the business associate" and to "perform data aggregation services"; and
- Business associate agreements also are still allowed to permit business associates to use PHI "to carry out the legal responsibilities of the business associate."

These provisions can be interpreted to allow business associates to utilize personal health information for purposes beyond those necessary to perform the service or function contracted for by the covered entity. Although no one has done a comprehensive study of BAAs or business associate use of data, there is some anecdotal evidence that expanded uses of information received from covered entities may be occurring.

For example, one large national business associate has been accused of using data it receives from covered entities to support other business objectives. Recently, CDT has reviewed an electronic health record vendor agreement that authorizes the vendor/business associate to use information from the EHR for any purpose not prohibited by HIPAA (e.g., not just acting on behalf of and at the direction of the provider). We also have heard anecdotal reports of a business associate agreement with a medical device manufacturer also authorizing the manufacturing to use information from the device for its own business purposes. The extent of this problem is not known, because, to the best of our knowledge, the HHS Office for Civil Rights (OCR) does not audit business associate agreements – and if such audits are occurring, the results have not been publicly shared.

3) Correct Implementation of Expanded Scope is Key

The expanded scope of accountability for compliance with HIPAA requires careful and correct implementation. We have concerns that business associates may interpret the expansion of

accountability in HITECH as providing them with the same legal status as a HIPAA covered entity – with full rights to access, use and disclose personal health information as a covered entity. Data received by a business associate to perform a particular service or function for a covered entity should not morph into information that the business associate may use and disclose for other purposes. The HIPAA regulations should provide the outer boundaries of permitted health information use and disclosure, but the BAA should be the tool to ensure that a business associate is permitted to use and disclose information only as reasonably necessary to perform the contracted services and functions.

To prevent the provisions enhancing business associate accountability from being a pipeline to broader uses and disclosures of personal health information, we call for stronger enforcement of HIPAA, as well as stronger federal oversight of business associates and BAAs. We further recommend that the Privacy Rule be revised to be crystal-clear that business associates and their contractors may use or disclose personal health information received from covered entities only for purposes explicitly enumerated in the business associate agreement, or required explicitly by law, and that these agreements should expressly limit the business associate’s access, use and disclosure of data.

4) Privacy and Security Tiger Team Recommendations

CDT’s recommendations are consistent with the August 2010 recommendations of the Privacy and Security Tiger Team of the Health IT Policy Committee, which were unanimously endorsed by the Committee. The recommendations urged the application of Fair Information Practice principles to third-party service organizations, like business associates, to promote trust in health information exchange. The Tiger Team recommended that third-party service organizations be permitted to collect, use, disclose, reuse or retain patient information only to the extent necessary to perform the functions specified in their service agreement or BAA and any administrative activities necessary to support those contracted functions.

Other applicable recommendations of the Tiger Team related to business associates include:

- Time limitation: Third-party service organizations should retain personally identifiable health information only for as long as reasonably necessary to perform the functions specified in the business associate or service agreement with the data provider, and necessary administrative functions. Retention policies for personally identifiable health information must be established, clearly disclosed to customers and overseen.
- Openness and transparency: Third party service organizations should be obligated to disclose in their business associate or service agreements with their customers how they use and disclose information, including without limitation their use and disclosure of de-identified data, their retention policies and procedures, and their data security practices.

In crafting these recommendations, the Tiger Team recognized that “[t]he exposure of a patient’s personally identifiable health information to third party service organization raises risk of disclosure and misuse, particularly in the absence of clear policies regarding that organization’s right to store, use, manipulate, re-use or re-disclose information.”

[Recommendations of the Privacy and Security Tiger Team of the Health IT Policy Committee](#) [4]

Conclusion

OCR should make clear in the Privacy Rule that (1) a BAA must expressly set forth the permitted access, use and disclosure of health information and (2) that a business associate’s access, use and disclosure of personal health information is limited to those expressly permitted by the BAA or required by applicable law. These limitations should also be expressly required to be carried forward

in subcontractor agreements and further limited if the scope of services to be provided by the subcontractor is narrower than the scope of the initial BAA. Patient privacy protection would be weak if the HIPAA Rules were the only real limitation on uses and disclosures of PHI by business associates and their subcontractors.

For more information, please contact Deven McGraw, Director, Health Privacy Project, deven@cdt.org [5]. CDT is grateful for the contributions of Alice Leiter, National Partnership for Women & Families, to this analysis.

Copyright © 2013 by Center for Democracy & Technology. All rights reserved. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://cdt.org/policy/rules-business-associate-agreements-need-clarification>

Links:

[1] http://www.cdt.org/files/pdfs/20090324_ARRAPrivacy.pdf

[2] http://cdt.org/files/pdfs/CDT_Comments_to_HHS_Proposed_Rulemaking_09-13-10.pdf

[3] <http://www.judiciary.senate.gov/pdf/11-11-9McGrawTestimony.pdf>

[4] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/hitpc_transmittal_p_s_tt_9_1_10.pdf

[5] <mailto:deven@cdt.org>