

January 11, 2010

HIPAA+HITECH Creates New Challenges for Covered Entities AND Business Associates

Stephen Siegel, Esq.

Buried within the American Recovery and Reinvestment Act of 2009 is the Health Information Technology for Economic and Clinic Health Act ("HITECH"). Much of HITECH is intended to promote the adoption and use of electronic health records by health care providers. However, some of HITECH's other provisions will have a significant impact on almost every HIPAA "covered entity" ("CE") and "business associate" ("BA"). The purpose of this article is to briefly review the impact of these provisions.

One of the changes HITECH makes is to mandate that a CE's business associate agreement impose an obligation on the BA to comply with HIPAA's privacy and security regulations. As a result, for many purposes, a BA will be treated as if it is a CE and have the same privacy and security obligations. Prior to HITECH, a BA only had a contractual obligation to protect a CE's protected health information ("PHI"); any breach of that obligation was a private matter between those parties.

Once the HIPAA+HITECH obligation to comply with the privacy and safety regulations becomes effective, on February 18, 2010, a breach of these regulations also will be enforceable by either the federal or state government (see below for a discussion of the enforcement authority HIPAA+HITECH grants to states). Every BA will be required to ensure that its policies, procedures, and operations comply with HIPAA's privacy and security regulations. These regulations provide, in part, that the entity (either a CE or a BA) appoint a chief privacy officer, implement an effective HIPAA compliance plan, implement physical and electronic measures, and adopt policies and procedures designed to protect the privacy and security of the PHI in its possession. **It is important to keep in mind that once information becomes protected health information, the obligation to protect its privacy and security attaches without regard to the form or form at (i.e., paper, digital, film) of that information.**

continued on page 2

The Health Law Practice Group

MIAMI

Brent Klein 305-789-2772

Stephen Siegel 305-789-2783

ORLANDO

William Sutton 407-244-8003

TAMPA

Debra Boje 813-222-6614

Bruce Lamb 813-222-6605

Mark Ragusa 813-222-6619

Brian Wright 813-222-6623

info@ruden.com

www.ruden.com

January 11, 2010

2

While HIPAA+HITECH will have a potentially significant impact on the operations and potential liability of every BA, CEs that contract with BAs also will need to respond to its requirements. Specifically, a CE will need to amend all of its business associate agreements in order to comply with HIPAA+HITECH. One question that remains unclear is whether a CE will have any obligation to ensure that its BAs actually adopt the measures and implement the policies and procedures required by HIPAA+HITECH.

Also effective February 18, 2010:

- CMS will be required to audit CEs in order to ensure that they are satisfying the requirements of HIPAA+HITECH. As a consequence, every CE needs to recognize the possibility that its HIPAA compliance plan, including its business associate agreements, will be audited and take steps to ensure that its plan is implemented, effective and fully compliant with HIPAA+HITECH.
- Patients will have the right to a copy of their PHI in either hard copy or an electronic format, if the covered entity maintains it as such.
- Health information exchanges, regional health organizations, e-prescribing gateways and other entities that provide electronic data transmission of PHI and require regular access to PHI will be considered to be covered entities and subject to the provisions of HIPAA+HITECH.

HIPAA+HITECH also includes some very significant enforcement/penalty provisions for CEs and BAs that fail to comply with HIPAA's requirements. Specifically:

- If HHS conducts a preliminary investigation of an alleged HIPAA violation and suspects that the violation was the result of willful negligence, the Department will be obligated to conduct a full investigation of the matter. Thus, it is likely the ability to quickly and inexpensively resolve HHS inquiries concerning alleged HIPAA violations will become more limited.
- CEs and BAs that are found to have willfully violated HIPAA can be subject to a fine of either \$10,000 or \$50,000 per violation, respectively (with a maximum fine of \$250,000 and \$1,500,000, respectively), depending on whether the violation has been corrected.
- If the BA/CE either did not know they were violating HIPAA or the violation was the result of a reasonable cause, the fines are limited to \$100 or \$1,000 per violation, with a cap of either \$25,000 or \$100,000, respectively.

continued on page 3

January 11, 2010

3

- Individuals who are harmed by HIPAA violations will be entitled to a portion of the amounts recovered in these enforcement actions. It seems probable that this change in the law will lead to a substantial increase in the number of alleged HIPAA violations that will be reported in the future.

State Attorneys General also will be authorized to bring HIPAA enforcement actions. If an enforcement action is successful, that state Attorney General can be awarded attorney's fees, making it much more likely states will undertake these enforcement actions. Between this provision and the right of a harmed individual to recover a portion of any recovery, we can expect to see HIPAA enforcement actions increase dramatically.

HIPAA+HITECH requires that any "breach" (i.e., an unauthorized use or disclosure of PHI that compromises its security or privacy) may have to be disclosed by the CE within 60 days after it is discovered. An independent contractor BA who discovers a breach will be obligated to notify the CE within a 60-day time period, or such lesser period as the parties' business associate agreement may require, so the CE can then make the necessary notifications. Depending on the nature of the breach, the CE may have to disclose it to the individual whose PHI has been compromised. In addition, depending upon the number of records that are included in a breach, the CE may be required to make disclosure to prominent local media outlets and/or the Department of Health and Human Services.

If it has not already done so, every CE should develop a database of its business associate agreements, amend all of its business associate agreements that will be effective on or after February 18, 2010, and review its HIPAA compliance plan in order to make whatever changes may be necessary in order to ensure the CE's compliance with this obligation after that date. Similarly, every BA should develop a database of its business associate agreements and ensure that all of them are amended appropriately. Further, if it has not already done so, a BA should begin adopting the policies and procedures and taking any other steps it may need in order to comply with the privacy and security regulations.

The purpose of this article has been to provide a very brief overview of the impact HIPAA+HITECH will have on CEs and BAs. Please keep in mind that in many respects HIPAA+HITECH is "as clear as mud" and there are many details and nuances which are still unclear. Compliance with this regulatory scheme is not as straightforward as the government would have you believe. Thus, it will be prudent for each CE and BA to involve its legal counsel and/or other parties who are familiar with HIPAA in its efforts to satisfy the HITECH amendments.

If you have questions regarding this topic contact Stephen Siegel, Esq., 305-789-2783 or stephen.siegel@ruden.com, or any Ruden McClosky health law attorney. Stephen Siegel is a partner in the Health Law Practice Group, in Miami, Florida. For more information about Ruden McClosky, please visit www.ruden.com.

[Boca Raton](#) • [Fort Lauderdale](#) • [Miami](#) • [Naples](#) • [Orlando](#) • [Port St. Lucie](#) • [Tallahassee](#) • [Tampa](#) • [West Palm Beach](#)