December 2012

Healthcare Entities, Cloud-Based IT Services, and Privacy Requirements

Healthcare providers and plans are increasingly moving to the cloud, in part because cloud services offer powerful tools at incredible value, including streamlining of administrative tasks and improved coordination of care. At the same time, a recent enforcement action by the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) makes clear that, when healthcare institutions avail themselves of the benefits of cloud computing, they must ensure their cloud service provider (CSP) is agreeable to taking proper safeguards for the protection of individually identifiable health information in compliance with the Health Insurance Portability and Accountability Act (HIPAA)[1] and the Health Information Technology for Economic and Clinical Health (HITECH) Act.[2] In the absence of such safeguards, healthcare entities could face potential liability under HIPAA.

In April 2012, Phoenix Cardiac Surgery, P.C., a small healthcare provider in Arizona, settled claims by OCR for, in part, "fail[ing] to obtain satisfactory assurances in business associate agreements from [its] Internet-based calendar and from [its] Internet-based public email providers that these entities would appropriately safeguard the [electronic protected health information] received from [Phoenix Cardiac Surgery]."[3] While the $100,000 settlement may seem modest to some, it makes clear that all healthcare entities, large and small, must be conscious of HIPAA and HITECH compliance obligations when selecting and working with a CSP.

I. A Cloud Computing Provider That Maintains Individually Identifiable Health Information on Behalf of a Covered Entity Is a Business Associate Under HIPAA.

HIPAA, including the HITECH amendments to it, places privacy and security obligations on "covered entities" and their "business associates."[4] Covered entities include health plans, healthcare clearinghouses, and healthcare providers that transmit any health information in electronic form in connection with a transaction covered by HIPAA.[5] A wide range of organizations are considered covered entities, including, but not limited to, hospitals, physician offices, academic medical centers, HMOs, medical service providers, government healthcare agencies, and even employer-sponsored group health plans.

Business associates include any person or entity, other than a member of a covered entity's workforce, that performs certain functions involving the use or disclosure of individually identifiable health information on behalf of, or that provides services to, a covered entity.[6]

---

[1] 42 U.S.C. §§ 1320d to 1320d-9 and implementing regulations at 45 C.F.R. Parts 160 and 164.

[2] 42 U.S.C. §§300jj *et seq.* and §§17901 *et seq.* and implementing regulations at 45 C.F.R. Parts 160 and 164.

[3] Resolution Agreement between HHS OCR and Phoenix Cardiac Surgery, P.C., (Apr. 11, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf.

[4] 45 C.F.R. § 160.102(a) (applicability of HIPAA); 42 U.S.C. §§ 17931 (applying security provisions to business associates) and 17934 (applying certain privacy provisions to business associates).

[5] 45 C.F.R. § 160.103 (definition of "covered entity").

[6] 45 C.F.R. § 160.103 (definition of "business associate").

HIPAA protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The HIPAA Privacy Rule calls this information "protected health information (PHI)."[7]

CSPs qualify as business associates under HIPAA when they host individually identifiable health information on behalf of a covered entity.[8] Representatives of OCR have stated on several occasions that such entities are business associates. The Phoenix Cardiac Surgery settlement demonstrates the risk that covered entities take when failing to treat them as business associates under HIPAA.[9]

II. Generally, a Covered Entity Will Not Comply with HIPAA Unless It Enters into a HIPAA-Compliant Business Associate Agreement with Its CSP.

The HIPAA Privacy Rule[10] requires a covered entity to obtain assurances from a business associate prior to disclosing PHI to the business associate or allowing the business associate to create or receive PHI on the covered entity's behalf.[11] Similarly, the HIPAA Security Rule[12] requires a covered entity to obtain assurances from a business associate prior to the covered entity permitting the business associate to create, receive, maintain, or transmit electronic PHI on the covered entity's behalf.[13] These assurances generally take the form of a written contract, or business associate agreement, between the covered entity and its business associate.[14]

Failure to sign a business associate agreement where one is required violates HIPAA and, like all HIPAA violations, is punishable by civil and criminal penalties.[15] Each day such a disclosure occurs may be a separate violation of the Privacy and Security Rules with civil penalties of up to $50,000 per violation and up to $1.5 million per calendar year for multiple violations of an identical provision.[16] Additionally, there can be significant damage to an entity's business reputation if the entity becomes the target of a government investigation.

A number of HHS/OCR settlements for HIPAA-related violations have exceeded $1 million. In 2012 alone, for example, HHS settled compliance matters with Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. ($1.5 million); Alaska Department of Health and Social Services ($1.7 million); and Blue Cross Blue Shield of

---

[7] 45 C.F.R. § 160.103 (definition of "protected health information").

[8] 45 C.F.R. § 160.103 (definition of "disclosure").

[9] *See* Phoenix Cardiac Surgery Resolution Agreement, *supra* note 3.

[10] Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, Subparts A & E.

[11] 45 C.F.R. § 164.502(e)(1).

[12] Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Parts 160 and 164, Subparts A & C.

[13] 45 C.F.R. § 164.308(b)(1).

[14] 45 C.F.R. §§ 164.314(a) and 164.504(e). Limited exceptions to the requirement to enter into a business associate agreement exist where, for example, both the covered entity and business associate are governmental entities.

[15] 45 C.F.R. §§ 164.308(b) and 164.502(e).

[16] 45 C.F.R. §§ 160.404(b)(2) (discussing civil money penalties) and 160.406 ("In the case of continuing violation of a provision, a separate violation occurs each day the covered entity is in violation of the provision").

Tennessee ($1.5 million).[17] As noted above, the settlement with Phoenix Cardiac Surgery shows that OCR is willing to enforce HIPAA even against smaller healthcare providers.

Further, the risks are not limited to OCR enforcement and reputational damage. State attorneys general also have the authority to enforce HIPAA.[18] Each state attorney general may seek damages with respect to health information of its residents of up to $100 per violation and up to $25,000 per calendar year for multiple violations of an identical provision.[19] For example, the Minnesota Attorney General settled a case earlier this year with Accretive Health, Inc., a debt collection agency, that alleged several HIPAA violations, including claims related to Accretive's alleged mining of patient data to determine ability to pay for current and future medical care.[20]

III. HIPAA-Specific Provisions Should Be Included in a Business Associate Agreement.

Among other provisions, CSPs should provide the following assurances to covered entities in a business associate agreement:

- Implementation of reasonable and appropriate administrative, physical, and technical safeguards as required by HIPAA;
- Limitation on uses and disclosures of the covered entity's PHI, including assurance that PHI will not be mined for the business associate's advertising or other commercial purposes or for any secondary purpose unrelated to providing cloud services to the covered entity;
- Notification to the covered entity's customers of any uses and disclosures that are not permitted under the business associate agreement, of security incidents, and of breaches of unsecured PHI; and
- Facilitation of the covered entity's ability to access, amend, and receive an accounting of disclosures with respect to their PHI.

IV. Conclusion

Covered entities can benefit from the cloud while complying with HIPAA. HIPAA compliance need not be an obstacle to obtaining the operational and cost efficiencies of cloud computing, but, to help avoid the risk of a costly HIPAA violation, covered entities should consider only CSPs that offer a HIPAA-compliant business associate agreement.

---

[17] For a list of Resolution Agreements since 2008, see www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

[18] 42 U.S.C. § 1320d-5(d).

[19] *Id*.

[20] *See State of Minn. v. Accretive Health, Inc.*, Second Amended and Supplemental Complaint, Civil File No. 12-145 RHK/JJK (D. Minn. June 19, 2012), *available at* htttp://www.ag.state.mn.us/PDF/Consumer/SecondAmendedSupplementaComplaint.pdf.