AFTER HITECH: HIPAA REVISIONS MANDATE STRONGER PRIVACY AND SECURITY SAFEGUARDS

VADIM SCHICK*

INTRODUCTION

Protection of personal information is emerging among the top priorities for college and university administrators. Congress and federal agencies are consistently strengthening requirements for safeguarding privacy and security of personal information.[1] Academic medical centers and all other

* Vadim Schick is an associate in the Information Technology and Data

institutions of higher education who are "covered entities" under the Health Insurance Portability and Accessibility Act of 1996 (HIPAA)[2] are particularly affected by this trend.[3]

The last two years saw the most dramatic increase in federal regulation of patient privacy since HIPAA was enacted in 1996. The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA), was primarily intended to incentivize the healthcare industry to switch from paper to Electronic Health Records (EHRs). It is a monumental effort, one which would not succeed without ensuring the privacy and security of Protected Health Information (PHI), as such protected data is defined under HIPAA, contained on the newly created digital records. Therefore, the HITECH Act also introduced substantial changes to HIPAA and the related regulations (including the HIPAA Privacy and Security Rules)[4] limiting covered entities' disclosure rights and mandating stronger safeguards for the safety and privacy of electronic PHI (e-PHI).

Colleges and universities are among the institutions most vulnerable to a data privacy breach.[5] According to the Department of Education, "[c]omputer systems at colleges and universities have become favored targets because they hold many of the same records as banks but are much

---

Protection Groups at the Washington, D.C., office of Post & Schell PC. Mr. Schick focuses on health information technology agreements and data privacy and security compliance. Mr. Schick received his B.A. in History and Russian Literature from Johns Hopkins University and his J.D. from Berkeley Law School. Mr. Schick served on the Board of Trustees of Johns Hopkins University from 2001 to 2005.

1. *See, e.g.*, Health Information Technology for Economic and Clinical Health ("HITECH") Act Pub. L. No. 111-5, §§ 13001–424, 123 Stat. 226 (2009). In fact, on December 1, 2010, the Federal Trade Commission released its findings on Internet privacy, along with a "privacy framework" which will include FTC's guidance regarding best practices in data protection; this privacy framework is expected to be the basis of a broader legislative action, championed by both Democratic and Republican members of Congress. *See, e.g.*, Edward Wyatt, *Agency Proposes Privacy as Default for Online Data*, N.Y. TIMES, (Dec. 1, 2010), *available at* http://www.nytimes.com/2010/12/02/business/media/02privacy.html?hp; Wendy Davis, Stearns' Privacy Bill Calls For Self-Regulation, FTC Oversight, Online Media Daily (Mar. 7, 2011), available at http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=146280.

2. Health Insurance Portability and Accessibility Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936.

3. *See* Joseph Goedert, *OCR Boosting Security Enforcement*, HEALTH DATA MANAGEMENT (May 12, 2010), http://www.healthdatamanagement.com/news/privacy_security-40268-1.html.

4. 45 C.F.R. 160, 164 (2010).

5. Mark Hrywna, *Nonprofits and Data Breaches*, NONPROFIT TIMES (July 1, 2007), *available at* http://www.nptimes.com/07Jul/npt-070701-2.html; Dan Toughey, *Consolidating Campus Commerce is All in the Cards*, http://www.touchnet.com/web/download/attachments/15433814/TouchNet_eBook .pdf (last visited Mar. 6, 2011).

easier to access."[6] In 2010, a significant portion of the major data breaches in the healthcare sector was reported by university hospitals and medical centers.[7] Georgetown University Hospital, NYU Hospital Center, University of San Francisco, and University of Florida are among many medical and research institutions which reported a data breach this year.[8] These breaches were reported to HHS because of the new breach notification mandates under the HITECH Act, which went into effect on September 23, 2009.[9]

While understanding and complying with the breach notification requirements should be a top priority for the institutions of higher learning subject to the rule, this article will focus on a different set of HITECH Act-related regulations. Pursuant to the HITECH Act, on July 14, 2010, the Secretary of Health and Human Services (HHS) issued the notice of proposed rulemaking mandating significant new safeguards for collection, storage, disclosures and disposal of PHI. This notice of proposed rule making will affect every institution of higher education which is also a HIPAA-covered entity or business associate. This paper cannot present a complete and exhaustive study of all the implications of the new HIPAA Privacy and Security rules for colleges and universities. However, it should provide a useful overview and summary of such updates, and alert the readers to the importance of ever-evolving and expanding regulatory protection for healthcare information privacy, as well as the heightened penalties for violation of such regulatory protections.

More specifically, Section I of this paper addresses applicability of HIPAA and the HIPAA Privacy and Security Rules ("HIPAA Rules") to post-secondary institutions. Section II examines the recent statutory and regulatory restrictions on collection, use and disclosure of PHI. Section III explores NPRM's updated enforcement provisions. Finally, Section IV focuses on the effects of the new regulatory environment on colleges and universities and suggests a few crucial practices and procedures that the affected organizations need to implement in order to comply with the new regulations.

I. APPLICABILITY TO COLLEGES AND UNIVERSITIES

A. HIPAA

HIPAA regulates "covered entities," which include health care providers

6. Family Educational Rights and Privacy; Final Rule, 73 Fed. Reg. 74,806, 74,843 (Dec. 9, 2008).

7. *Breaches Affecting 500 or More individuals*, Office of Civil Rights, Department of Health and Human Services, *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

8. *Id.*

9. *See* 45 C.F.R. 160, 164 (2010).

who transmit any health information in electronic form, health plans, and health care clearinghouses.[10] The HIPAA Privacy and Security Rules oblige covered entities to safeguard the privacy of PHI and to honor security standards regarding patient information maintained in electronic form.[11] The HITECH Act extended many of the requirements of HIPAA and HIPAA Rules to business associates, which include persons and organizations performing functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of PHI.[12]

Colleges and universities mostly fall under the category of "covered entities" under HIPAA, either as health care providers or as health plans. However, colleges or universities and medical centers can also act as business associates in instances where such entities provide services to health care providers, including health information exchange (HIE) or similar data sharing or storage services. In turn, college and university medical centers and hospitals who are HIPAA covered entities engage many business associates including outsourced IT services providers, vendors of EHR and other healthcare IT technology, data processors and many other related organizations.

B. FERPA vs. HIPAA

Any university with a medical school, medical center, hospital, or a university health insurance plan most likely qualifies as a covered entity. Perhaps less obviously, some schools with on-campus clinics may be subject to the HIPAA rules also. Student clinics at colleges and universities are not necessarily subject to HIPAA and the related HIPAA Rules. The Family Educational Rights and Privacy Act[13] ("FERPA") applies to most public and private postsecondary institutions and to the education records of the students of such institutions. Student treatment records fall under "education records" and are governed by FERPA, rather than HIPAA.[14] For example, notes from a college or university psychologist's treatment of a student are not subject to HIPAA Rules, but to the relevant privacy rule under FERPA.[15] However, most institutions of higher education operate on-campus clinics not only for their students but

10. 45 C.F.R. § 164.501 (2010).

11. 45 C.F.R. §§ 160, 164 (2010).

12. 45 C.F.R. § 160.103 (2006); HITECH Act, Pub. L. No. 111-5, § 13401(a), 123 Stat. 241, 260 (2009).

13. 20 U.S.C. § 1232g; 34 C.F.R. pt. 99 (2010).

14. *See* 45 C.F.R. §§ 160.103(2)(i), (2)(ii) (2010) (exceptions to the definition of "protected health information").

15. *See* U.S. DEP'T OF HEALTH AND HUMAN SERVS., FREQUENTLY ASKED QUESTIONS: DOESFERPA OR HIPAA APPLY TO RECORDS ON STUDENTS AT HEALTH CLINICS RUN BY POSTSECONDARY INSTITUTIONS? http://www.hhs.gov/ocr/privacy/hipaa/faq/ferpa_and_hipaa/518.html (last visited Feb. 24, 2011).

also for employees, staff, faculty, members of the local community, or the public in general. HIPAA Rules will apply to the protected health information of all nonstudents and such institutions will be "subject to both *HIPAA* and *FERPA* and . . . are required to comply with *FERPA* with respect to the health records of their student patients, and with the *HIPAA* Privacy Rule with respect to the health records of their *non*student patients."[16]

HHS further clarified that FERPA will apply to students treated at university hospitals only if the university hospital operates the clinic or treats the student *on behalf* of the university.[17] More commonly, if the university hospital is treating the student as any patient, regardless of their status as a student at the university, their records will be subject to the HIPAA Privacy Rule.[18] While a detailed discussion of FERPA is outside of the scope of this paper, it is worth pointing out that the major difference between application of FERPA and HIPAA is that HIPAA, including the HIPAA Rules, requires a much higher level of data protection safeguards than FERPA's non-binding recommendations;[19] and, unlike FERPA, the HIPAA Rules now include far-reaching breach notification mandates.[20]

C. Hybrid Entities

Finally, some colleges and universities will qualify as "hybrid entities" under the HIPAA Rules.[21] A hybrid entity is a single legal entity which is a covered entity, whose business activities include both covered and non-covered functions; and that designates the health care component in accordance with 45 C.F.R. §160.504(c)(3)(iii).[22] A hybrid entity must designate any component that would meet the definition of a covered entity as if it were a separate legal entity, but such designation is purely internal (although it must be in writing and accessible if audited by HHS).[23] A hybrid entity must ensure that its health care component complies with the applicable provisions of the HIPAA Rules, including, *inter alia*, not disclosing PHI to another component of the covered entity if the Rule

16. *Id.*

17. U.S.DEP'T OF HEALTH AND HUMAN SERVS., FREQUENTLY ASKED QUESTIONS: DOES FERPA OR HIPAA APPLY TO RECORDS ON STUDENTS WHO ARE PATIENTS AT A UNIVERSITY HOSPITAL?, *available at* http://www.hhs.gov/ocr/privacy/hipaa/faq/ferpa_and_hipaa/519.html (last visited Feb. 24, 2011).

18. *Id.*

19. Family Educational Rights and Privacy, 73 Fed. Reg. 74,806, 74,843–44 (Dec. 9, 2008) (describing the non-binding nature of the Department of Education's recommendations on breach notification and implementing privacy and security safeguards to protect educational records).

20. 45 C.F.R. § 164.404 (2011).

21. 45 C.F.R. § 164.103 (2010) (definition of "hybrid entity").

22. 45 C.F.R. §§ 164.103, 164.504 (2010).

23. 45 C.F.R. §§ 164.105(a)(iii)(C), 164.105(c)(i) (2010).

would prohibit such disclosure if the two components were separate and distinct legal entities and protecting e-PHI as if the two components were separate and distinct legal entities.[24]

II. HITECH ACT AND HHS REGULATIONS

The HITECH Act includes numerous measures aimed to strengthen patient privacy safeguards and protections, including new breach notification requirements, limitations on disclosures of PHI, significant increases in penalties, and greater enforcement efforts by HHS. In this paper, however, we will focus on only a few key changes included in the HITECH Act and expanded upon in the regulations issued by the Office of Civil Rights (OCR) of the Department of Health and Human Services on July 14, 2010 (2010NPRM).[25] OCR has jurisdiction over both HIPAA Privacy and HIPAA Security Rules, after the responsibility for enforcement of the Security Rule was transferred to OCR from the Centers for Medicare and Medicaid Services on August 3, 2010.[26]

A. New Requirements and Restrictions Regarding Disclosures of PHI

1. Disclosures to a Health Plan

While individuals could request certain restrictions on the use or disclosure of their PHI, covered entities were not obligated to accept such requests under the original HIPAA Privacy Rule.[27] However, § 13405 of the HITECH Act restricts a covered entity's right to refuse an individual's request not to use or disclose such individual's PHI in instances where "the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment);" and the PHI "pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full."[28]

OCR's comments in the 2010 NPRM expose some of the practical difficulties that providers will encounter in complying with this rule. OCR solicited comments on whether and how health care providers must notify pharmacies (especially as e-prescribing becomes more and more prevalent) and subsequent treating providers of such restriction by the patient.[29] The 2010 NPRM also references situations where a patient may not be able to

24. 45 C.F.R. §§ 105(a)(ii)–(iii) (2010).

25. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the HITECH Act, 75 Fed. Reg. 40,868 (July 14, 2010) [Hereinafter 2010 NPRM]..

26. Press Release, U.S. Dep't of Health and Human Servs., *HHS Delegates Authority for the HIPAA Security Rule to Office for Civil Rights*, *available at* http://www.hhs.gov/news/press/2009pres/08/20090803a.html.

27. 45 C.F.R. §§ 164.522(a)(1)(i)-(ii).

28. HITECH Act, Pub. L. No. 111-5, , §§ 13401(a), 13405(a), 123 Stat. 241, 260, 264 (2009).

29. 2010 NPRM, 75 Fed. Reg. at 40,899.

pay for a procedure or service out-of-pocket (e.g., instances where providers are paid by an HMO).[30]

The HITECH Act requires covered entities to account for disclosures of PHI even to carry out treatment, payment and health care operations. All such disclosures must be accounted for if the disclosure was made "through an electronic health record."[31] However, HHS has delayed issuing regulations on this major new mandate, thereby leaving it out of the scope of this paper.[32]

2. "Minimum Necessary" Disclosure Standard

Section 13405 of the HITECH Act also requires covered entities, when using or disclosing PHI, or requesting PHI from another covered entity, to limit "to the extent practicable" disclosure of PHI to the "limited data set" as defined under HIPAA,[33] or, if more information is "needed," to the minimum necessary "to accomplish the intended purpose of such use, disclosure, or request, respectively[.]"[34] The Act retains all the current exceptions to the existing minimum necessary disclosure standard (including disclosures made for treatment purposes and disclosure required by law)[35] and does not apply to use, disclosure or request of de-identified PHI.[36] The Act calls on HHS to issue guidance defining the "minimum necessary" standard, but the 2010 NPRM merely requests comments on such standard.[37]

3. No Sale of PHI Without Authorization

Both the HITECH Act and the 2010 NPRM mandate that covered entities obtain an individual's authorization prior to selling (or receiving remuneration for) his or her PHI.[38] Importantly, OCR decided not to require covered entities to state in the authorization whether PHI will be sold in the future because the recipient of such PHI would have to obtain an authorization prior to selling this PHI again.[39] The Act and OCR carve out eight exceptions with respect to disclosures of PHI for:

---

30. 2010 NPRM, 75 Fed. Reg. 40,868, 40,900 (July 14, 2010).

31. HITECH Act, § 13405(c)(1), 123 Stat. at 266; 45 C.F.R. § 164.528(a)(1)(i) (2010).

32. *See, e.g.*, HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act; Request for Information, 75 Fed. Reg. 23,214 (May 3, 2010).

33. 45 C.F.R. § 164.514(e)(2) (2006).

34. HITECH Act, Pub. L. No. 111-5 § 13405(b)(1)(A), 123 Stat. 241, 264–65 (2009).

35. *Id.* at § 13405(b)(3), 123 Stat. at 265.

36. *Id.* at § 13405(b)(4), 123 Stat. at 265.

37. 2010 NPRM, 75 Fed. Reg. 40,868, 40,896(July 14, 2010).

38. HITECH Act, § 13405(d), 123 Stat. at 267.

39. 2010 NPRM, 75 Fed. Reg. at 40,890–91.

1. Public Health activities (as defined under HIPAA), including a covered entity's or business associate's disclosure PHI in a "limited data set" for public health purposes;[40]
2. Research, if the price paid for PHI reflects the costs of preparation and transmission of PHI;[41]
3. Treatment and payment purposes;[42]
4. Sale, transfer, merger or consolidation of all or part of the covered entity and due diligence related to such activity,[43] as well as health care operations;[44]
5. Activities that the covered entity's business associate undertakes covered by an applicable business associate agreement;
6. Providing an individual with a copy of the individual's PHI pursuant to HIPAA regulation 164.524;[45]
7. To comply with applicable laws;[46] and
8. Instances where remuneration to the covered entity or business associate does not exceed the cost of preparing and transmitting such PHI.[47]

The HITECH Act also limits a covered entities' ability to use PHI for marketing purposes, with certain exceptions including for treatment of the individual and case management and care coordination, and allows patients to opt-out of receiving certain marketing communications.[48] Furthermore, the HITECH Act and the 2010 NPRM require covered entities sending fundraising communications to provide recipients with a "clear and conspicuous" opportunity and a "simple, quick, and inexpensive way" to opt-out of receiving future communications, explaining that such opting-out will not affect future treatment of the individual.[49] While such additional restrictions are outside the scope of this paper, they serve as a worthy reminder about the strengthening regulatory grip over healthcare

40. *Id.* at 40,891.

41. OCR requested comments to determine such "costs." *Id.*.

42. OCR added "for payment purposes" to make sure that paying for treatment does not qualify as a "sale" of PHI. 2010 NPRM, 75 Fed. Reg. 40,868, 40,891 (July 14, 2010).

43. 45 C.F.R. § 164.501 (2010) (found under definition of "health care operations" (6)(iv)).

44. 2010 NPRM, 75 Fed. Reg. at 40,891.

45. 45 C.F.R. 164.524 (2010) ("Access of Individuals to Protected Health Information").

46. 2010 NPRM, 75 Fed. Reg. at 40,892.

47. *Id.*

48. HITECH Act, Pub. L. No. 111-5, § 13406, 123 Stat. 241, 268 (2009).

49. 2010 NPRM, 75 Fed. Reg. 40,868, 40,896(July 14, 2010)), *citing in part*, HITECH Act, § 13406(b).

providers' handling of protected patient data.

B. Access to PHI Contained in an EHR

Upon a patient's request, the HITECH Act requires covered entities to produce a copy of such patient's PHI in electronic format, and if the individual so chooses, to transmit the copy directly to an entity or person designated by the individual, provided the request is "in writing, signed by the individual, and clearly identif[ies] the designated person and where to send the copy of protected health information."[50] The Act limits the fee a covered entity may charge the patient for such an electronic record to the labor costs in responding to the request for the copy (or summary or explanation).[51] The 2010 NPRM broadens the applicability of this rule to all e-PHI, regardless of whether it is stored in an EHR.

OCR's comments make it clear that OCR expects a covered entity or business associate to provide the patient with a copy of his or her e-PHI if it is readily producible, or, if not, in a readable electronic format as agreed to by both parties (e.g., e-mail, secure web-based portal, USB drives or other portable electronic media). Interestingly, OCR requires covered entities to safeguard the shared e-PHI, meaning providing copies only via secure portals or on encrypted disks or other storage media. OCR also allows a covered entity to charge the requesting patient for the cost of an encrypted USB drive containing his or her PHI.[52] However, "if an individual requests that an electronic copy be sent via unencrypted e-mail, the covered entity should advise the individual of the risks associated with unencrypted e-mail, but the covered entity would not be allowed to require the individual to instead purchase a USB flash drive."[53]

It is also worth noting that providing patients with copies of their PHI is not only a requirement under HIPAA, it is also an important objective for those college and university medical centers or hospitals seeking to achieve "meaningful use" in order to capitalize on the HITECH Act's significant incentives for "meaningful" EMR users, as defined in the HITECH Act and the related HHS regulations.[54] The relevant metric requires that eligible hospitals and professionals provide at least "50 percent of all patients who request an electronic copy of their health information . . . within 3 business

50. *Id.* at 40,902.

51. HITECH Act, § 13405(e), 123 Stat. at 268 (2009).

52. 2010 NPRM, 75 Fed. Reg. at 40,902.

53. *Id.* The access requirement drew much attention in February 2011 when OCR issued its first fine for willful neglect of this requirement. This case is addressed in greater detail in Section III.

54. *See, e.g.*, Medicare and Medicaid Programs; Electronic Health Record Incentive Program, 75 Fed. Reg. 44,314. (July 28, 2010). While this is an additional point regarding the importance of providing access to patients' PHI, a detailed discussion of meaningful use and the HITECH incentives is outside the scope of this note.

days."[55]

C. Business Associate Provisions

As mentioned above, the HITECH Act extends many of the requirements under HIPAA and HIPAA Rules to business associates of covered entities.[56] The 2010 NPRM expands the definition of "business associate" even further to include health information organizations, patient safety organizations, personal health record vendors acting on behalf of a covered entity, e-prescribing gateways, and subcontractors of business associates.[57] Under the 2010 NPRM, "subcontractors" means persons who act "on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate."[58] More specifically, subcontractors who create, receive, maintain, or transmit PHI fall under the expanded definition of business associate.[59]

Importantly, OCR also weighed in regarding those entities which are *not* business associates. OCR clarified that the following common transactions, among others, do not give rise to a business associate relationship: conduits for transport of PHI (with only random or infrequent access to PHI);[60] PHI disclosures from one covered entity to another provider about treatment;[61] PHR vendors offering PHRs not on behalf of a covered entity (which, though not under HHS's regulation, are still subject to the FTC's jurisdiction pursuant to the HITECH Act); and health plan disclosures to plan sponsors.[62]

OCR requires subcontractors of business associates to enter into business associate agreements (BAAs) with business associates (similar to the ones between covered entities and business associates), but clarifies that the HIPAA Rules apply to such subcontractors regardless of the existence of such a business associate agreement.[63] Thus, covered entities do not have to enter into separate agreements with subcontractors.[64]

The new regulations also require a number of changes in the BAAs themselves. Some of the required provisions include:

1. Requiring the business associate to comply with the HIPAA

55. *Id.* at 44,567.

56. HITECH Act, Pub. L. No. 111-5, § 13401(a), 123 Stat. 241, 260 (2009).

57. 2010 NPRM, 75 Fed. Reg. 40,868, 40,912 (July 14, 2010) (definition of "business associate") (to be codified at 45 C.F.R. § 160.103).

58. *Id.* at 40,913 (definition of "subcontractor") (to be codified at 45 C.F.R. §160.103).

59. *Id.* at 40, 912.

60. *Id.* at 40,873.

61. *Id.* at 40,912.

62. 2010 NPRM, 75 Fed. Reg. 40,868, 40,912 (July 14, 2010).

63. *Id*. at 40,887–88.

64. *Id.* at 40,888.

Security Rule;[65]

2. Requiring business associates to report security incidents and breaches of PHI to the covered entity (which also applies downstream, to the business associate-subcontractor agreements);
3. Ensuring that the business associate obtains a BAA with its relevant subcontractors and that such BAA will have the same terms as the BAA between the covered entity and such business associate; and
4. A termination right for the covered entity in the event the business associate breaches the BAA or violates HIPAA; the same termination requirement should apply downstream, to the business associate's agreements with its subcontractors.[66] (It is worth noting here that each BAA should contain a provision requiring the business associate to return all PHI to the covered entity, in the format requested by such covered entity, upon termination of the agreement, regardless of the reason for such termination).

OCR allows covered entities, business associates and their subcontractors a one-year reprieve from the compliance date of the revised rules to continue operating under existing contracts.[67] Section IV will provide a brief discussion regarding the importance of updating existing BAAs or negotiating new ones, including certain terms with regard to liability, cost allocation and indemnification.

D. Compound Authorizations for Research

Perhaps of particular note for research universities and medical centers is OCR's proposed modification regarding conditioned and unconditioned authorizations for clinical research. The HIPAA Privacy Rule bans "compound authorizations" (i.e., where PHI-related authorization is combined with any other legal permission).[68] This presents a problem for clinical researchers trying to obtain a single authorization that covers use or disclosure of PHI for a research study which includes both a clinical trial and bio-specimens banking (or "tissue-banking") for future research. The current rule requires covered entities to either restrict the stored PHI to a "limited data set" or obtain multiple authorization forms from the patient-subject. The first option is troublesome because it may negatively affect the very purpose of the study by removing important, relevant information about an individual. The second option is also flawed because, as OCR pointed out, clinical trials may involve thousands of participants, and storing two sets of authorizations is a major concern, and could potentially

65. *Id.* at 40,919–21.
66. *Id.*
67. *Id.* at 40,889–90 .
68. 2010 NPRM, 75 Fed. Reg. 40,868, 40,892 (July 14, 2010) *citing* 45 C.F.R. § 164.508(b)(3)(i)) (2009).

confuse the subject.[69]

Responding to such concerns, OCR proposed to allow covered entities to combine a conditioned authorization for use of PHI in a clinical trial with an unconditioned authorization permitting inclusion of the individual's PHI in a central repository, providing covered entities some flexibility with respect to how they meet this authorization requirement.[70] OCR offered several examples of how a covered entity could design an effective authorization and solicited comments on any additional ways to achieve the same result. OCR's examples included:

1. "describing the unconditioned research activity on a separate page of a compound authorization[;]"
2. "[cross-referencing] relevant sections of a compound authorization to minimize the potential for redundant language[;]"
3. "us[ing] a separate check-box for the unconditioned research activity to signify whether an individual has opted-in to the unconditioned research activity, while maintaining one signature line for the authorization[;]" and
4. "[providing] a distinct signature line for the unconditioned authorization to signal that the individual is authorizing optional research that will not affect research-related treatment."[71]

However, if a provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, any compound authorization "must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization."[72]

Furthermore, OCR is soliciting comments regarding authorizations for future research use or disclosure of PHI, including with respect to the HIPAA Privacy Rule's requirement to use or disclose PHI only for a specific purpose (which is sometimes referred to as the "specificity requirement").[73] OCR agreed to reconsider the specificity requirement in light of the comments and recommendations of an HHS advisory committee.[74]

Even if OCR loosens the requirement for obtaining authorization for each subsequent research use of PHI, an individual will always have the right to revoke such authorization at any time, and the applicable

69. *Id*. at 40,893.
70. *Id*. at 40,892–93.
71. *Id*. at 40,893.
72. *Id*. at 40,921.
73. 2010 NPRM, 75 Fed. Reg. 40,868, 40,894 (July 14, 2010).
74. *Id.*

authorization will have to tell the individual how to do so.[75]

E. Student Immunization Records

The 2010 NPRM allowed covered entities to send a student's or prospective student's immunization records to schools upon request (which does not have to be in writing) of such student's parent or guardian, but only if the school requires proof of immunization in accordance with applicable state or other laws.[76] OCR is soliciting comments regarding a wide range of issues: defining the meaning of "school," including whether post-secondary institutions should fall under this definition; applicability of FERPA to the immunization records once in possession of the school; and whether oral request (rather than written authorization) is sufficient for the covered entity to provide immunization records.[77]

III. ENFORCEMENT

The HITECH Act introduced a number of very significant changes to HIPAA's Enforcement Rule.[78] These HITECH-mandated changes, including the increased and tiered civil money penalties, were the subject of an interim final rule released in the Federal Register on October 30, 2009.[79] While a detailed discussion of the enforcement interim final rule is beyond the scope of this article, it is worthwhile to review a few key changes to the Enforcement Rule mandated by the HITECH Act:

1. HHS is required to formally investigate any complaint where a preliminary investigation of the facts indicates a possible violation of the HIPAA Rules due to willful neglect, and to impose a penalty in those cases where a violation is found;[80]
2. Any civil money penalty or monetary settlement collected under the HIPAA Rules must be transferred to OCR, and a percentage of such civil money penalties and monetary settlements must be distributed to harmed individuals;[81]
3. The Act dramatically increased the civil money penalty structure

75. *Id.*

76. *Id.* at 40,922 (to be codified at 45 C.F.R. pt. 164).

77. *Id.* at 40,895–96.

78. The "Enforcement Rule" outlines the covered entities' responsibilities with respect to cooperation in the enforcement process, provides rules governing the investigation by HHS of such compliance, establishes rules governing the process and grounds for establishing the amount of a civil money penalty, and provides procedures for hearings and appeals where the covered entity challenges HHS's finding of a violation. *See* 2010 NPRM, 75 Fed. Reg. 40,868, 40,869 (July 14, 2010).

79. HIPAA Administrative Simplification: Enforcement,74 Fed. Reg. 56,123 (Oct. 30, 2009).

80. 2010 NPRM, 75 Fed. Reg. at 40,870.

81. *Id.*

for violations of the HIPAA Rules occurring after February 18, 2009. Such civil money penalties are tiered based on culpability. This provision is already in effect, and has been since February 18, 2009. The new civil money penalties range from a minimum of $100 for each violation the covered entity or business associate did not know about, to a minimum of $50,000 for each violation which such covered entity or business associate willfully neglected and failed to correct, all with an annual (January 1st through December 31st) cap of $1,500,000.[82] Table 1 of the interim final rule summarizes the penalties;[83]

Violation Category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect—Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected	50,000	1,500,000

Table 1—Categories of Violations and Respective Penalty Amounts Available

4. Also in effect as of February 18, 2009, state attorneys general now have the authority to enforce the HIPAA Rules on behalf of their states' residents.[84]

The 2010 NPRM discussed herein does not modify the interim final rule, which is now in effect, but clarifies the interpretation of a few important provisions, including:

1. As of February 18, 2010, business associates are subject to the Enforcement Rule "in the same manner" as the covered entities, including for actions of such business associates' agents or subcontractors;[85]
2. In cases involving willful neglect, HHS *must*, as opposed to may, impose a civil money penalty (as opposed to mandating a corrective action plan);[86]
3. The definitions of "reasonable cause" and "willful neglect" applicable to covered entities' or business associates' actions are

82. HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56,123, 56,127–28. (Oct. 30, 2009).

83. *Id.* at 56,127.

84. *Id.*

85. 2010 NPRM, 75 Fed. Reg. 40,868, 40,875 (July 14, 2010).

86. *Id.* at 40,876.

clarified.[87] "Reasonable cause" is modified to mean "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect."[88] The new definition makes it possible for a covered entity or business associate to know that it is violating the rule, but not be subject to willful neglect penalties. Noncompliance does not rise to the level of willful neglect when, for example, such organization exercises ordinary care and prudence in trying to comply, or when the organization lacks the *means rea* or reckless indifference to complying with the applicable regulations;[89]

4. An exception to a covered entity's liability for violations of the HIPAA Rules caused by its business associates in cases where a compliant BAA was in place between the two organizations is stricken, thereby imposing an additional burden on the covered entity to make sure its business associates, agents and subcontractors are performing their duties;[90] and
5. The nature of the violation and the nature of the harm caused by such violation are added to the list of factors determining the scope of a covered entity's or business associate's culpability with respect to a violation of the HIPAA Rules.[91]

These high numbers described above are no longer empty threats. On February 22, 2011, HHS imposed the first civil money penalty on a covered entity pursuant to the HIPAA Privacy Rule.[92] HHS fined Cignet Health, a Maryland health plan and healthcare provider, $1.3 million for violating the rights of 41 patients by denying them access to their medical records after repeated requests in 2008 and 2009. HHS imposed an additional $3 million dollar civil money penalty on Cignet for failing to cooperate in the agency's investigation of such claims.[93]

Even more surprising and ominous, however, was the settlement HHS

87. 2010 NPRM at 40,877–78.

88. *Id.*

89. *Id.* at 40,878–79. OCR provides a number of very helpful examples for what constitutes "reasonable cause" or "reasonable diligence" or "willful neglect." *Id*. However, a more detailed discussion of this subject is beyond the scope of this article.

90. 2010 NPRM, 75 Fed. Reg. 40,868, 40,879 (July 14, 2010).

91. *Id.* at 40,880–81.

92. HHS Press Release, *HHS Imposes a $4.3 million civil penalty for violation of the HIPAA Privacy Rule* (Feb. 22, 2011), *available at* http://www.hhs.gov/news/press/2011pres/02/20110222a.html.

93. *Id. See also* Notice of Final Determination (Feb. 4, 2011), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cignetpenaltyletter.pdf.

reached that same week with Massachusetts General Hospital ("MGH"). MGH agreed to pay HHS $1 million for 192 lost patient records from its infectious diseases clinic.[94] Such records contained sensitive personally identifiable data, including HIV/AIDS status and patients' insurance information, and were lost when an MGH employee left them on a subway train.[95] In its investigation, HHS found that MGH did not adopt adequate privacy and security safeguards for protected information when such data have been removed from the hospital's premises.[96] Unlike Cignet, the MGH example presents a much more realistic and foreseeable situation for many university hospital centers, and should serve as a reminder to all covered entities to safeguard PHI at and outside the healthcare provider's premises and the significance of training of each member of such provider's staff in the patient privacy protection. This should also serve as a wake-up call for even the most sophisticated institutions that civil money penalties under HIPAA are not just hypothetical.

It is also vital to keep in mind that even the harshest civil money penalties do not represent the total cost of a data breach or HIPAA violation to colleges and universities subject to such regulations. The costs of investigations and audits, calculated both in terms of dollars spent and hours dedicated, can easily exceed the amount of fines imposed by HHS. As discussed in Section IV, below, taking affirmative steps to ensure compliance and protecting the school contractually will go a long way in easing this regulatory burden and reducing (though not necessarily eliminating) the likelihood of a HIPAA violation or breach at your school.

IV. IMPLICATIONS FOR COLLEGES AND UNIVERSITIES

If made final, the amendments discussed in Section II will have significant practical implications for those institutions of higher education that qualify as "covered entities" or "business associates" under HIPAA. While by no means exhaustive, the list below should highlight some of the obligations and next steps for such colleges and universities to prepare for HIPAA compliance in advance of the effective date of the new rules. Eligible schools should keep in mind that many of the changes discussed in Section II are mandated by the HITECH Act. Therefore, even though HHS has not produced the final regulations regarding privacy and security of patient information, compliance with the *statutory* portions of updates to HIPAA is unavoidable.

94. HHS Press release, *Massachusetts General Hospital Settles Potential HIPAA violations* (Feb. 24, 2011), *available at* http://www.hhs.gov/news/press/2011pres/02/20110224b.html.

95. *Id.*

96. *Id.*

A. Determine Eligibility

As discussed in Section I, some post-secondary institutions are not "covered entities" or "business associates" under HIPAA. Yet even if some colleges and universities are not subject to HIPAA, a plethora of other data privacy laws may apply to such institutions. For example, FERPA applies to students' educational records; GLBA[97] and the Payment Card Industry Data Security Standards[98] apply to financial and credit card information that the college or university collects, uses or stores; and state data privacy laws (most notably in such states as California, which enacted strict data protection and breach notification laws[99]) apply to the personal information of the organization's employees, applicants, and board members.

B. Assess Current Privacy Policies and Procedures

Covered entities and business associates (especially those organizations which fall under the newly expanded definition of the latter) must review their HIPAA policies and procedures to ensure they comply with the HIPAA Rules as recently amended by the HITECH Act and the resulting regulations.

Such assessments should include, but should not be limited to:

1. The administrative, physical, and technical safeguards protecting PHI resident on the school's servers or in another form of electronic media, especially if such media (e.g., laptops, USB drives, CDs) can be taken out of the covered entity's premises;
2. Practices with regard to collection of data from students, applicants, patients, and employees;
3. Practices with regard to disclosure of PHI to a health plan in the event a patient requests restricting such disclosure and pays for the relevant service out-of-pocket;
4. Whether any sale of PHI is restricted to only the eight exceptions proposed in the 2010 NPRM (keeping in mind that at least six of such exceptions are statutory);
5. Any affect of the new rules easing bans on compound authorizations for research use, including exemptions affecting tissue-banking and possible elimination of the specificity requirement;
6. Marketing and fundraising practices, especially if the college and university is using patient data to solicit donations;

97. Grahm, Leach, Blily Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999.)

98. *See* Payment Card Industry Security Standards Council, https://www.pcisecuritystandards.org/.

99. *See, e.g.*, CAL. CIV. CODE §§ 1798.80–84 (West 2010); CAL. HEALTH & SAFETY CODE, § 1280.15 (West 2010).

7. Policies and practices around requesting or providing student immunization records;
8. Staff's (especially staff with access to protected health information) familiarity with applicable laws and required procedures;
9. School's preparedness for a breach, including existence of an incident response plan; and
10. Risk analysis mandated by the HIPAA Security Rule and the analysis of all gaps identified in such assessment.[100]

After performing the assessment, the school should implement the required changes in a timely manner, and, if necessary, provide additional data protection safeguards, including encrypting the protected data (which removes it from the coverage of most breach notification laws), and limiting initial collection of personal information (on the principle that one cannot lose what one does not have). Colleges and universities should follow the HIPAA Security Rule's requirements of limiting access by staff to data systems based on their role in the organization, thereby preventing unauthorized or unnecessary downloading, printing, or e-mailing of protected data.

Training employees in data protection is absolutely critical to safeguarding PHI and other protected personal information. Intentional data breaches at university hospitals or the affiliated hospital systems are often inside jobs. For example, Huping Zhou, a former employee at the UCLA Healthcare System, plead guilty to federal charges of breaches of patient privacy.[101] Zhou accessed the UCLA patient records system 323 times during a three-week period, mostly looking for the files of celebrities, after being let go by the hospital.[102] On April 27, 2010, Zhou was sentenced to four months in prison after pleading guilty to four misdemeanor counts of HIPAA violations, thereby becoming the first person ever sentenced to prison for violating HIPAA.[103] In a similar incident at UCLA Medical Center, in 2008, nurse Lawanda Jackson "pleaded guilty to selling medical-records information to a tabloid. Her targets reportedly included Britney Spears and Farrah Fawcett."[104]

Finally, each school should have a data breach response plan and team in place to ensure a coordinated, quick and comprehensive response to a data

100. 45 C.F.R. § 160.308(a)(1)(ii)(A).

101. Bill French, *Former UCLA Healthcare Worker Sentenced to Prison for Snooping*, NBC LOS ANGELES, April 28, 2010, http://www.nbclosangeles.com/news/local-beat/Former-UCLA-Healthcare-Worker-Sentenced-Prison-Snooping-92265634.html.

102. Dennis Romero, *Former UCLA Health Worker Pleads Guilty To Accessing Celebrities' Medical Records*, L.A. WEEKLY, January 8, 2010, *available at* http://blogs.laweekly.com/informer/city-news/ucla-health-worker-pleads-guil.

103. French, *supra* note 101.

104. Romero, *supra* note 102.

breach. The response team should be tasked with, *inter alia*, discovering what information the school possesses and its location; content of the lost data, and determining all applicable laws.

C. Review Business Associate Agreements

Both covered entities and business associates should systematically review all business associate agreements for compliance with the HITECH Act's changes to HIPAA and the HIPAA Rules. Prior to the effective date of the updated HIPAA Rules (and, indeed, prior to OCR issuing the final regulations), each new BAA should include a provision where the parties acknowledge that the terms and conditions of such BAA remain subject to any changes mandated by the upcoming final rules issued by HHS pursuant to the HITECH Act. After review, covered entities should include the newly required provisions discussed in Section II.C above, including compliance with the Security Rule and clauses regarding termination rights and return of PHI upon such termination.

Colleges and universities should pay particular attention to the provisions governing liability for violations or breaches of HIPAA or the HIPAA Rules. Costs associated with breaches of PHI, and HIPAA violations more broadly, may be very substantial because such costs include expenses associated with forensic investigations, notification of affected individuals, and attorney and consultant fees. Business associates should indemnify covered entities for all such costs resulting from a breach caused by the business associate or its subcontractors. If business associates absolutely refuse to accept this indemnification obligation, then at minimum, the BAA should provide for the party responsible for the breach or HIPAA violation to compensate or indemnify the non-breaching party, and any damages resulting from such obligation should not be subject to a general limitation of liability clause in the master or license agreement between the two entities. For example, if a business associate health IT vendor causes a major breach (e.g., loses tapes containing PHI), and the covered entity must conduct investigations, hire attorneys, and then notify its patients, the health IT vendor should indemnify the covered entity and bear the costs associated with such a breach and such costs should be specifically carved out from any applicable cap on damages. Under no circumstances should a college or university agree to indemnify their vendors or business associates, especially in cases where such indemnification provisions may affect the school's insurance coverage.[105]

105. While discussion of insurance if outside the scope of this article, it is important to note that many insurance contracts will not cover any costs or damages associated with an indemnification obligation assumed by the insured. In instances where healthcare providers obtained privacy and security insurance coverage, insurance professional within or outside your organization should review the legal provisions regarding liability and indemnification in the BAA and the underlying agreement.

D. Confidentiality Clauses in Vendor Agreements

BAAs are often a part of a broader, "master" agreement between a medical center and its vendor-business associate. It is important to keep in mind that each school should know its vendors and their practices, and attempt to ensure through contractual obligations that such vendors use secure technology when handling sensitive data. Most standard vendor contracts contain terms protecting the vendor's trade secrets and restricting access to the software. However, it is rare to find similar protections for the healthcare provider. Providers should insist on mutual confidentiality obligations with strict limitations on the vendor's use of the organization's patient information. Some vendors insist on obtaining the right to use patient data for their internal data analytics purposes. Even if vendors promise to collect or use only limited data sets of such PHI, healthcare providers should make sure that vendors indemnify them for any breaches or losses occurring as a result of such use. However, any such data use should be carefully examined, and the agreement should clearly delineate each party's rights and responsibilities with respect to collection, maintenance, use, destruction and return of PHI upon termination of such agreement.

This is especially important in light of changes to the existing HIPAA regime, as mandated by the HITECH Act and the accompanying regulations. Privacy and security issues are directly related to a provider's ability to amend and/or terminate the contract for a vendor's failure to comply with applicable laws, fair allocation of compliance costs, and requirements for vendors to enter into business associate agreements, where applicable. Healthcare providers changing their existing BAAs with vendors should also review and assess the relevant provisions in the underlying "master" or license agreements with such vendors.

E. Providing Copies of e-PHI

Schools should have the ability to provide a patient with a secure electronic copy of his or her e-PHI upon written request by the patient and in a format requested by the patient. This will likely require some consideration and preparation, including assessing current practices, reviewing the institution's EMR, PHR, or other technological capabilities, creating a set of procedures and assigning staff to procure such e-copies, and training such staff in these procedures. As mentioned previously, providing patients with access to their e-PHI is also one of the core objectives for achieving "meaningful use" under the HITECH Act's incentive payment program for adoption of electronic health records.[106]

106. Medicare and Medicaid Program; Electronic Health Record Incentive Program, 75 Fed. Reg. 44,314, 44,370–722 (July 28, 2010) (to be codified at 42 C.F.R. 412, 413, 422, 495).

This will be especially crucial for those university hospitals seeking to achieve meaningful use and capitalize on the HITECH Act incentives.

V. CONCLUSION

Post-secondary education institutions should pay close attention to the evolving regulatory landscape in data privacy protection. The federal government considers protection of patient information a high priority, and continues to mandate additional safeguards. This is particularly true of information stored in electronic format or on electronic health records because the government looks to health IT to improve patient care and achieve major cost savings. A hospital, medical center or any other covered entity or business associate within or affiliated with a college or a university, should review and revise their existing data privacy and security policies and procedures to both comply with the new regulations as they become effective, and to achieve a broader policy goal of keeping the personal information in their possession private and secure.