2023

Privacy for Student-Patients: A Call to Action

Stacey A. Tovino, *University of Oklahoma College of Law*

PRIVACY FOR STUDENT-PATIENTS: A CALL TO ACTION

Stacey A. Tovino[*]

Consider a law student who has a mental or reproductive health issue that the student wishes to keep private. If the student seeks care at an off-campus health clinic that is not affiliated with the student's law school or university, the student typically has a number of federally enforceable privacy rights. For example, the federal HIPAA Privacy Rule will typically apply and prohibit the clinic from disclosing the student's protected health information to professors, parents, and other third parties without the student's prior written authorization. The law student also will have the right to receive a notice of privacy practices, the right to request further privacy restrictions, the right to obtain paper and electronic copies of medical records, the right to amend incorrect medical record entries, the right to receive an accounting of medical record disclosures, the right to ask privacy-related questions of an institutional privacy officer, and the right not to be intimidated, threatened, coerced, or discriminated against for exercising these rights. The HIPAA Security Rule also will typically apply, requiring the clinic to implement administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of the student's electronic protected health information. Finally, if the off-campus clinic discovers a breach of the student's unsecured protected health information, the HIPAA Breach Notification Rule will typically apply, requiring the clinic to report the breach to the student, the federal government and, in certain cases, prominent media outlets serving the jurisdiction.

If the law student seeks care at a health center affiliated with the student's university, however, the story will be completely different. This is because the medical records that result from the student's encounter with the student health center—called student treatment records—are excepted from the definition of protected health information under the HIPAA Privacy, Security, and Breach Notification Rules. Student treatment records also are excepted from the definition of education records under the Family Educational Rights and Privacy Act of 1974 (FERPA), the major federal statute that requires federally funded academic institutions to protect the privacy of such records. These exceptions exist because Congress, in late 1974, expressed its intent that student treatment records be protected only by state law. Unfortunately, state law provides minimal protections for student treatment records.

This Article responds to the need for greater privacy, security, and breach notification protections for student treatment records. After reviewing a number of privacy and security breaches involving colleges and universities and the patchwork of federal and state law that fails to adequately protect student treatment records, this Article shows that many student health centers provide students with confusing information (at best) and misleading or incorrect information (at worst) regarding their privacy, security, and breach notification protections. After providing several practical, political, and health policy justifications for amending federal law, this Article re-writes relevant statutory and regulatory provisions in FERPA and HIPAA. If the proposals set forth in this Article are implemented by the federal government, student treatment records will receive the maximum privacy, security, and breach notification protections available currently available under the law.

TABLE OF CONTENTS

INTRODUCTION

Consider a 23-year-old law student who has a mental or reproductive health issue that the student wishes to keep private.[1] If the student seeks care at an off-campus health clinic that is not affiliated with the student's law school or university, the student typically has a number of federally enforceable privacy rights.[2] For example, the federal HIPAA Privacy Rule will prohibit the clinic from disclosing the student's protected health information (PHI) to professors, parents, and other third parties without the student's prior written authorization.[3] Clinic personnel cannot even mention that the student received care without the student's express consent.[4] The student also will have the right to: (1) receive a notice of privacy practices, (2) request additional privacy protections, (3) receive paper and electronic copies of medical records, (4) request amendment of incorrect medical record entries, (5) receive an accounting of medical record

* William J. Alley Professor of Law and Faculty Director, Graduate Healthcare Law Programs, The University of Oklahoma College of Law, Norman, Oklahoma. The Author thanks Dean Katheleen Guzman for her generous financial support of this project; Ms. Taylor Crossley for her meticulous research assistance; and Mr. Kenton Brice, Ms. Elaine Bradshaw, Mr. Sam Gorme, Mr. Kale Parker, and Ms. Becca Schmidt for their resource assistance. The Author also thanks the organizers and participants of the following meetings, conferences, and lectures for their comments and suggestions on the ideas presented in this Article: Southeastern Association of Law Schools (SEALS) Annual Meeting, Sandestin, Florida (July 2022); American College of Legal Medicine (ACLM) and American Board of Legal Medicine (ABLM) Mid-Year Conference, Oklahoma City, Oklahoma (October 2022); Association of American Law Schools (AALS) Annual Meeting, San Diego, California (January 2023); and the Nova Southeastern University Shepard Broad College of Law Guest Lecture (January 2023).

[1] *See, e.g.*, Charles Ornstein, *When Students Become Patients, Privacy Suffers*, PROPUBLICA (Oct. 23, 2015), https://www.propublica.org/article/when-students-become-patients-privacy-suffers (reporting the story of a Yale University student who sought mental health care and wanted to keep care private).

[2] *See infra* text accompanying notes 3–12 (summarizing rights enforceable under the HIPAA Privacy, Security, and Breach Notification Rules); *infra* Part I.A (carefully reviewing rights enforceable under the HIPAA Privacy, Security, and Breach Notification Rules); Ornstein, *supra* note 1 (noting correctly "[i]f a student seeks help off campus or at a university hospital, HIPAA, the more-restrictive law, typically applies").

[3] The HIPAA Privacy Rule is a federal health information confidentiality regulation promulgated pursuant to the Administrative Simplification provisions within the Health Insurance Portability and Accountability Act of 1996 (HIPAA). *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (Aug. 21, 1996) (codified at 45 C.F.R. §§ 164.501–.534 (2021)) (directing HHS to promulgate national privacy regulations if Congress fails to enact timely privacy legislation). The HIPAA Privacy Rule applies to covered entities, including health care providers that transmit health information in electronic form in connection with certain standard transactions. 45 C.F.R. § 160.103 (2021) (defining covered entity). A health clinic that submits an electronic health insurance claim to an insurer meets the definition of a covered entity. *Id.* The HIPAA Privacy Rule prohibits covered entities from disclosing a patient's protected health information without the patient's prior written authorization unless the disclosure is otherwise permitted or required by the Privacy Rule. *Id.* § 164.508(a)(1).

[4] 45 C.F.R. § 160.103 (2021) (defining protected health information (PHI) with reference to health information (HI), where the definition of HI includes "any information" that relates to "the provision of health care to an individual").

disclosures, (6) ask privacy-related questions of an institutional privacy officer, and (7) not be intimidated, threatened, coerced, or discriminated against for exercising these rights.[5] The HIPAA Security Rule also will apply, requiring the clinic to implement administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of the student's electronic protected health information (ePHI).[6] Finally, if the off-campus clinic discovers a breach of the student's unsecured protected health information (uPHI), the HIPAA Breach Notification Rule will apply, requiring the clinic to report the breach to the student, the federal government and, in certain cases, prominent media outlets serving the jurisdiction.[7]

If the off-campus clinic violates any of these rights or requirements, the student may complain to the federal Department of Health and Human Services (HHS),[8] which can provide technical assistance, require corrective action, and/or impose civil monetary penalties as high as $1,919,173.[9] Regulations soon may be promulgated that would allow the student to share in any civil monetary penalties imposed by HHS.[10] HHS also can refer the clinic to the federal Department of Justice (DOJ), which can impose criminal penalties as high as $250,000 and/or imprisonment for up to ten years.[11] If the federal government declines to exercise its enforcement authority, the relevant state attorney general is permitted to bring a civil action against the clinic enjoining further HIPAA

---

[5] *See id*. §§ 164.520–.530 (codifying these rights); *infra* text accompanying notes 114–31 (discussing these rights in more detail).

[6] 45 C.F.R. §§ 164.302–.318 (2021) (codifying the HIPAA Security Rule); *infra* Part I.A.2 (defining ePHI and summarizing administrative, physical, and technical safeguards set forth in HIPAA Security Rule).

[7] 45 C.F.R. §§ 160.400–.414 (2021) (codifying the HIPAA Breach Notification Rule); *infra* Part I.A.3 (defining uPHI and summarizing the individual, governmental, and media notification requirements set forth in the HIPAA Breach Notification Rule).

[8] 45 C.F.R. § 160.306 (2021) (establishing process pursuant to which individuals may file privacy and security related complaints with Secretary of HHS).

[9] 42 U.S.C. § 1320d-5 (2018) (setting forth civil penalties applicable to HIPAA Rules violations); Annual Civil Monetary Penalties Inflation Adjustment, 87 Fed. Reg. 15100, 15101, 15109 (Mar. 17, 2022) (updating these penalties for calendar year 2022 based on inflation); *infra* Part I.A.4 (explaining how the federal government enforces the HIPAA Rules).

[10] Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended, 87 Fed. Reg. 19833, 19838 (Apr. 6, 2022) (soliciting public comment on the distribution of civil penalties and monetary settlements to individuals harmed by HIPAA Privacy violations).

[11] 42 U.S.C. § 1320d-6 (2018) (setting forth criminal penalties applicable to HIPAA Privacy Rule violations); *Enforcement Process*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html (last visited Feb. 5, 2023) (illustrating HIPAA Privacy and Security Rules enforcement process).

Rules violations, obtaining civil damages on behalf of the student, and seeking reimbursement for legal costs.[12]

If the law student seeks care at a health center affiliated with the student's university, however, the story will be completely different. This is because the medical records that result from the student's encounter with the student health center—called student treatment records—are excepted from the definition of PHI under HIPAA.[13] Student treatment records also are excepted from the definition of education records under the Family Educational Rights and Privacy Act of 1974 (FERPA),[14] the major federal statute that requires federally funded academic institutions to protect the privacy of such records.[15] These exceptions exist because Congress, in late 1974, expressed its intent that student treatment records be protected only by state law.[16]

---

[12] American Recovery and Reinvestment Act, Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5 § 13410(e), 123 Stat. 226, 271–74 (2009) (codified at 42 U.S.C. § 1320d-5(d) (2010)).

[13] 45 C.F.R. § 160.103 (2021) (excluding from the definition of PHI "records described at 20 U.S.C. § 1232g(a)(4)(B)(iv);" that is, student treatment records).

[14] 20 U.S.C. § 1232g(a)(4)(B)(iv) (2023) (excepting from the definition of FERPA-protected education records "records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice").

[15] *See, e.g.*, 34 C.F.R. § 99.1(a) (2021) (stating FERPA "applies to an educational agency or institution to which funds have been made available under a program administered by the Secretary [of the U.S. Department of Education]"); *Family Educational Rights and Privacy Act (FERPA)*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/phlp/publications/topic/ferpa.html (last updated July 27, 2022) (explaining that private schools at the elementary and secondary level typically do not receive funding under a program administered by the U.S. Department of Education and, therefore, are not regulated by FERPA; further explaining, however, that most private postsecondary schools do receive such funding and are subject to FERPA); Student Press L. Ctr. v. Alexander, 778 F. Supp. 1227, 1228 (D.D.C. 1991) (explaining FERPA's purpose as "ensur[ing] access to educational records for students and parents and to protect the privacy of such records from the public at large" and noting that FERPA "conditions federal education funding" on the institution's ability to "maintain[] the privacy of education records") (internal quotation marks omitted) (citations omitted).

[16] *See* S. REP. No. 93-1409, at 10 (1974) (Conf. Rep.) (explaining, in FERPA's legislative history, that FERPA was not designed to "alter the confidentiality of communications otherwise protected by law . . . [because s]tate laws and court decisions var[ied] so widely that the . . . potential effects [of FERPA if it did regulate student treatment records] were uncertain . . . [and could] disrupt existing [state-level] parental and student rights to confidentiality"); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82483 (Dec. 28, 2000) (stating that HHS chose not to protect student treatment records under HIPAA because doing so would be "inconsistent with the policy in FERPA that these records be exempt from regulation to the extent the records were used only to treat the student").

State law, however, is not a robust source of privacy, security, or breach notification protections.[17] Traditionally, states have had extraordinarily limited—and extremely uneven—protections for health information.[18] Even though a handful of states have enacted new consumer data protection laws that apply to health information and grant patients additional privacy, security, and/or breach notification rights, these laws tend to exclude educational institutions from regulation and student treatment records from protection.[19] When all is said and done, the result is minimal privacy, security, and breach notification protections for the treatment records of postsecondary students, including the law student described in the opening of this Article.[20]

That federal law does not protect the privacy and security of student treatment records is curious given that undergraduate and graduate students, including those who have crossed jurisdictional lines to attend out-of-state institutions, are heavily encouraged by faculty, staff, and other university personnel to seek mental health, reproductive health, infectious disease, and other sensitive health services on campus, at the student health center.[21] Indeed, college, graduate, and professional students are flooded with emails, flyers, brochures, and other communications that identify services available at the student health center and that advertise confidential appointments for such services.[22] Rarely do these university-sponsored communications clarify the privacy, security, and breach notification costs to students of seeking care at a student health center rather than an independent, off-campus health care facility.[23] To the contrary, many students are provided a HIPAA Notice of Privacy Practices at the beginning of their first student health center visit.[24] Frequently, this notice will state or suggest that student treatment records are

---

[17] *See infra* Parts I.C.1–6 (explaining why state law is not a robust source of protections for student treatment records).

[18] *See infra* Parts I.C.1–6 (reviewing potential state law sources of student treatment record protections and explaining why most of these sources are extraordinarily limited in terms of substance or are inapplicable altogether); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82466 (Dec. 28, 2000) (describing state privacy law as a "patchwork" that is "incomplete and, at times, inconsistent . . . with considerable variation among the states in the type of information protected and the scope of the protections provided").

[19] *See infra* Part I.C.6.

[20] *See infra* Parts I.A–C.

[21] *See infra* Part III.

[22] *See infra* Part III.

[23] *See infra* Part III.

[24] *See infra* Part II.

protected by HIPAA and that students have federally enforceable rights in the event of a privacy or security breach when the opposite is true.[25]

That federal law does not protect the privacy and security of student treatment records is also concerning given the stigma, shame, and prejudice associated with many physical and mental health conditions for which postsecondary students seek treatment.[26] Sexually transmitted infections (STIs) remain heavily stigmatized, even in an era of sex positivity,[27] and STI-related stigma and shame have been found to undermine STI testing, treatment, and partner notification.[28] Mental health conditions and substance use disorders are also associated with significant shame, stigma, and prejudice that can interfere with diagnosis, treatment, and recovery.[29] In both contexts, public health experts recommend strengthening privacy and security protections as a means of

[25] *See infra* Parts I.A–B, II.

[26] *See, e.g.*, Nassim Bickham, *The Stigma of Seeking Mental Health Care for College Students*, TIMELYCARE (Aug. 26, 2022), https://timelycare.com/blog/the-stigma-of-seeking-mental-health-care-for-college-students/ (reporting that six out of ten college students have a mental health condition and that many college students do not seek the help they need due to stigma); Karen R. Barth et al., *Social Stigma and Negative Consequences: Factors That Influence College Students' Decisions to Seek Testing for Sexually Transmitted Infections*, 50 J. AM. COLL. HEALTH 153, 153–58 (2010) (investigating why college students delay or avoid seeking testing for sexually transmitted infections even if the services are readily available; finding that social stigma represents a significant barrier to willingness to be tested, which could increase students' risk of spreading infections).

[27] *See* Jen Gunter, *Why Sexually Transmitted Infections Can't Shake Their Stigma*, N.Y. TIMES (Aug. 13, 2019), https://www.nytimes.com/2019/08/13/style/sti-stigma-sexual-transmitted-infections.html ("[T]he sexual revolution stopped short of liberating people from the shame and stigma of sexually transmitted infections.").

[28] *See, e.g.*, Jessica L. Morris et al., *Sexually Transmitted Infection Related Stigma and Shame Among African American Male Youth: Implications for Testing Practices, Partner Notification, and Treatment*, 28 AIDS PATIENT CARE & STDS 499, 500 (2014) (stating that sexually transmitted infection-related stigma and shame can undermine STI testing, treatment, and partner notification programs).

[29] *See, e.g.*, Jeffrey Borenstein, *Stigma, Prejudice and Discrimination Against People with Mental Illness*, AM. PSYCH. ASS'N (Aug. 2020), https://www.psychiatry.org/patients-families/stigma-and-discrimination (explaining that mental health-related stigma is associated with treatment reluctance); *Reframing Shame: Everyone Wins When We Dismantle Stigma*, NAT'L INST. HEALTH, https://heal.nih.gov/news/stories/reframing-shame ("Widespread lack of information and understanding about mental or substance use disorders can lead to public attitudes of shame and blame. Stigma is a well-recognized barrier for people with mental illness, leading many to avoid prevention or treatment programs."); Bernice A. Pescosolido et al., *Trends in Public Stigma of Mental Illness in the US, 1996–2018*, 4(12) JAMA 1 (Dec. 21, 2021) (studying mental illness-related stigma in the United States between 1996 and 2018 and reporting a decrease in the stigma associated with depression but increases or stabilized stigma in association with other mental health conditions).

combating screening and treatment hesitancy.[30] Yet, student treatment records remain protected only by weak and uneven state law.[31]

The lack of federal protections for student treatment records also must be weighed against current political realities. In June 2022, the Supreme Court of the United States issued its opinion in *Dobbs v. Jackson Women's Health Organization*, holding that the U.S. Constitution does not explicitly or implicitly establish a right to an abortion[32] and that the issue should remain in the hands of state lawmakers.[33] Since *Dobbs*, thirteen states have criminalized most abortions, and Georgia has banned abortions at approximately six weeks.[34] Given states' increasing regulation and criminalization of reproductive health care, the confidentiality of postsecondary students' reproductive health information is more important than ever.[35]

Advances in technology also weigh in favor of strong privacy, security, and breach notification protections for student treatment records. Paper medical records were the norm in 1974, the year Congress passed FERPA and expressly

---

[30] *See, e.g.*, Jami S. Leichliter et al., *Confidentiality Issues and Use of Sexually Transmitted Disease Services Among Sexually Experienced Persons Aged 15–25 Years*, 66 MORBIDITY & MORTALITY WEEKLY REP. 237 (2017) ("Public health efforts to reduce confidentiality concerns [in the context of individuals aged 15 to 25 who seek STI services] might be useful. Some medical organizations suggest that providers have time alone with patients without a parent in the room."); *Reducing Stigma*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/mentalhealth/stress-coping/reduce-stigma/index.html (last updated July 22, 2021) ("Community leaders and public health officials can help prevent stigma by . . . [m]aintaining the privacy and confidentiality of those seeking healthcare and those who may be part of any contact investigation."). *See generally* Sarah Clement et al., *What Is the Impact of Mental Health-Related Stigma on Help-Seeking? A Systematic Review of Quantitative and Qualitative Studies*, 45 PSYCH. MED. 11, 21 (2015) (reporting that disclosure and confidentiality concerns seem to be the most prominent type of stigma barrier to mental health help-seeking).

[31] *See infra* Parts I.C.1–6 (finding that state privacy, security, and breach notification protections for student treatment records are weak and uneven).

[32] Dobbs v. Jackson Women's Health Org., 597 U.S. __, *5 (2022) ("The Constitution makes no reference to abortion, and no such right is implicitly protected by any constitutional provision[.]") (internal references and citations omitted).

[33] *Id.* at *6 ("It is time to heed the Constitution and return the issue of abortion to the people's elected representatives.").

[34] *See Tracking the States Where Abortion Is Now Banned*, N.Y. TIMES, https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html (last updated Dec. 12, 2022) (reporting states' increasingly strict abortion regulations and prohibitions post-*Dobbs*).

[35] *See, e.g.*, Stacey A. Tovino, *Confidentiality Over Privacy*, 44 CARDOZO L. REV. 1243, 1246 (2023) (examining a range of confidentiality issues involving reproductive health information post-*Dobbs*); Kayte Spector-Bagdady & Michelle M. Mello, *Protecting the Privacy of Reproductive Health Information After the Fall of* Roe v, Wade, 3(6) JAMA HEALTH F. e222656 (June 30, 2022) (asking, post-*Dobbs*, how clinicians and facilities can protect their patients and themselves from having reproductive health information used against them).

excluded student treatment records from federal protection.[36] Although it is not impossible to breach the privacy and security of paper records, electronically maintained information is particularly vulnerable to large-scale breaches followed by widespread (and unauthorized) uses, disclosures, and/or sales.[37] Smart phones, also not available in 1974, have increased the ease with which a student's health information can be quickly photographed, screenshotted, emailed, texted, voiced, or videoed by a worker (including a student worker) at a student health center and disclosed to an unauthorized third party (including other students) or spread via social media.[38] Today's new digital landscape begs for greater privacy, security, and breach notification protections for student treatment records.[39]

Notwithstanding, on-campus health centers frequently violate patient privacy and data security.[40] In one example, a student health center affiliated with Yale University disclosed a student's mental health information to her parents without her prior written authorization.[41] The disclosure occurred even though the student, named Andrea, was over the age of majority[42] and even though personnel at the Yale Health Center knew that Andrea had a broken relationship with her parents and that Andrea's mother refused to acknowledge her daughter's serious mental health condition.[43] Indeed, after Andrea's parents were notified of Andrea's mental health condition without Andrea's prior

---

[36] *See* Family Educational Rights and Privacy Act, Pub. L. No. 93-380, § 513, 88 Stat. 571–74 (1974) (codified at 20 U.S.C. § 1232g); R. S. Evans, *Electronic Records: Then, Now, and in the Future*, IMIA YEARBOOK MED. INFORMATICS S48, S48 (2016) (reporting that the inadequacies of paper medical records became increasingly apparent by 1992, when the Institute of Medicine advocated a shift from a paper-based to an electronic medical record).

[37] *See, e.g.*, Vincent Liu et al., *Data Breaches of Protected Health Information in the United States*, 313 JAMA 1471, 1472 (2015) (investigating the characteristics and scope of health data breaches in the United States and finding that most breaches occurred via electronic media and involved laptop computers or portable electronic devices); *infra* text accompanying notes 48–56 (referencing large-scale security breaches involving university-owned ePHI).

[38] *See generally* Deborah Ng, *Smile! You're on my Cell Phone: Camera Phones and Privacy*, LEGALZOOM (July 12, 2022), https://www.legalzoom.com/articles/smile-youre-on-my-cell-phone-camera-phones-and-privacy (examining the extent to which smart phone cameras can be involved in violations of personal privacy).

[39] *See* David Grande et al., *Health Policy and Privacy Challenges Associated With Digital Technology*, 3(7) JAMA NETWORK OPEN e208025 (2020) (discussing the impact of digital technology on patient privacy and concluding that sector-specific privacy regimes are insufficient to protect patient privacy).

[40] *See infra* notes 41, 47–48, 52–56 and accompanying text.

[41] *See* Ornstein, *supra* note 1.

[42] *See id.* (stating that Andrea was no longer a minor).

[43] *See* Christina Cauterucci, *At Universities, Students Medical Records Are Open Territory*, SLATE (Oct. 23, 2015), https://slate.com/human-interest/2015/10/university-students-have-little-right-to-privacy-in-medical-records.html.

authorization, they refused to allow her to access further mental health care.[44] If Andrea had presented to an off-campus health clinic not affiliated with Yale University, the HIPAA Privacy Rule would have prohibited the clinic from notifying Andrea's parents and Andrea would have remained in treatment.[45]

Although the incident at Yale University involved just one student, a number of public and private universities have experienced significant privacy and security breaches that have involved the identifiable health information of thousands of patients.[46] In 2010, for example, the University of Pittsburgh Student Health Center experienced a major privacy and security breach when papers and films containing the uPHI of 8,000 patients were lost or stolen.[47] In 2013, by further example, a malware infection of a University of Massachusetts Amherst (UMass) workstation resulted in the unauthorized disclosure of the ePHI of 1,670 patients.[48] A subsequent government investigation revealed that UMass's failure to implement policies and procedures designed to protect the privacy and security of PHI, failure to conduct an accurate and thorough security risk analysis, and failure to implement technical security measures contributed to the breach.[49] A similar security breach occurred at Oklahoma State University (OSU) in 2016 and 2017, when an unauthorized third party gained access to an OSU web server and installed malware that resulted in the disclosure of 279,865 patients' ePHI, including their names, dates of birth, addresses, and treatment information.[50] A subsequent government investigation revealed that OSU had failed to conduct an accurate and thorough security risk analysis, failed to implement audit controls, and failed to comply with security incident response and reporting requirements.[51] Significant privacy and security breaches also have occurred at hospitals, clinics, and other health care facilities affiliated with

---

[44] *Id*.

[45] *See* Ornstein, *supra* note 1 ("If Yale's health center hadn't shared information about her condition with her parents . . . she would have moved in with a friend or a friend's family while seeking continued treatment.").

[46] *See infra* notes 47–56 (referencing privacy and security breaches involving thousands of patients).

[47] U.S. DEP'T OF HEALTH & HUM. SERVS., BREACH PORTAL ARCHIVE, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf# (last visited Aug. 13, 2023) (listing the University of Pittsburgh Student Health Center as reporting a breach involving the uPHI of 8,000 individuals).

[48] *See* Resolution Agreement between U.S. Department of Health and Human Services and The University of Massachusetts Amherst ¶2 (Nov. 16, 2016), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/umass/index.html (summarizing privacy and security failures at UMass).

[49] *Id*.

[50] *See* Resolution Agreement between U.S. Department of Health and Human Services and Oklahoma State University–Center for Health Sciences (OSU-CHS) ¶2 (May 5, 2022), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/osu-ra-cap/index.html (summarizing these privacy and security failures).

[51] *Id*.

Idaho State University,[52] Oregon Health and Science University,[53] University of Mississippi,[54] and University of Rochester,[55] among hundreds of other academic institutions.[56] This Article responds to the need for greater privacy, security, and breach notification protections at postsecondary institutions, focusing in particular on protections needed for student treatment records.

This Article proceeds as follows: Part I reviews potentially relevant federal privacy, security, and breach notification laws, showing how most postsecondary student treatment records are excluded from protection.[57] Part I also provides a comprehensive review of state facility licensing laws, state medical record privacy laws, state data security laws, state breach notification laws, and new state consumer data protection laws, explaining why these state laws provide minimal (if any) protections for student treatment records.[58] The result is that most student treatment records are protected only by antiquated privacy provisions set forth in state professional practice acts.[59] Part I reveals that these state professional practice acts: (1) do not carefully or heavily regulate the use and disclosure of student treatment records; (2) do not provide students with comprehensive rights relating to their health information, including the right to receive a notice of privacy practices, the right to request additional

---

[52] *See* Resolution Agreement between U.S. Department of Health and Human Services and Idaho State University (May 13, 2013), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/idaho-state-university/index.html (summarizing privacy and security failures at Idaho University).

[53] *See* Resolution Agreement between U.S. Department of Health and Human Services and Oregon Health and Science University ¶2 (July 18, 2006), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ohsu/index.html (summarizing privacy and security failures at Oregon Health and Science University).

[54] *See* Resolution Agreement between U.S. Department of Health and Human Services and University of Mississippi Medical Center ¶2 (July 7, 2016), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ummc/index.html (summarizing privacy and security failures at the University of Mississippi).

[55] *See* Resolution Agreement between U.S. Department of Health and Human Services and University of Rochester Medical Center ¶2 (Oct. 30, 2019), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/urmc/index.html (summarizing privacy and security failures at the University of Rochester).

[56] *See generally* U.S. DEP'T OF HEALTH & HUM. SERVS., BREACH PORTAL ARCHIVE, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf# (listing 178 uPHI breaches that were reported by universities).

[57] *See infra* Parts I.A–B; *infra* note 176 (explaining why HIPAA, FERPA, and Federal Trade Commission (FTC) rules do not protect most student treatment records).

[58] *See infra* Parts I.C.2–6 (explaining why state facility licensing laws, state medical record privacy laws, state data security laws, state breach notification laws, and new state consumer data protection laws do not protect most student treatment records).

[59] *See infra* Part I.C.1 (reviewing the vague and antiquated protections available for student treatment records under state professional practice acts).

privacy protections, the right to correct inaccurate medical record entries, the right to receive an accounting of disclosures, the right to be notified of privacy and security breaches, or the right to mitigation of harmful effects associated with such breaches; (3) do not require the implementation of administrative, physical, or technical safeguards designed to ensure the confidentiality, integrity, and availability of student health information; and (4) are not aggressively enforced (or enforceable) through stringent civil and criminal penalties, qui tam provisions, or private rights of action.[60]

Part II of this Article explores whether postsecondary institutions make their students aware that their treatment records lack strong federal protections and/or suffer from weak state protection.[61] Part II finds that student health centers inform postsecondary students of privacy, security, and breach notification protections through a variety of means, including through specific statements made in notices of privacy practices; general statements made on health center and other university web pages; and cursory language in emails flyers, brochures, posters, and other materials (collectively health center communications). Part II reveals that many health center communications provide postsecondary students with confusing information (at best) and misleading or incorrect information (at worst). In particular, Part II shows that many health center communications: (1) fail to adequately distinguish between the significant protections available for the medical records of non-students and the limited protections available for student treatment records;[62] or (2) incorrectly state or suggest that all student health center patients have stringent protections.[63] After providing several health policy justifications for amending federal law, Part III re-writes relevant provisions in FERPA and HIPAA to better protect student treatment records.[64] If these proposals are implemented by the federal government, all student treatment records will be protected by the HIPAA Privacy, Security, and Breach Notification Rules at all times, thus receiving the maximum protection currently available in federal or state law.[65]

---

60 *See infra* Part I.C.1.
61 *See infra* Part II.
62 *Infra* Part II.A.
63 *Infra* Part II.B.
64 *Infra* Part III.
65 *Infra* Part III.

I. PRIVACY, SECURITY, AND BREACH NOTIFICATION LAW

Although a variety of federal and state laws contain data privacy, security, and breach notification protections, most of these laws do not apply to student treatment records.[66] As discussed in more detail below, the federal HIPAA and FERPA regimes exclude most postsecondary student treatment records from the definitions of protected health information and education records, respectively.[67] In addition, state medical practice acts, state facility licensing laws, state medical record privacy laws, state data security laws, state breach notification laws, and new state consumer data protection laws either do not apply to student treatment records or provide marginal (if any) protections for such records.[68] As a result, postsecondary students have substantially inferior privacy, security, and breach notification protections compared to non-students.

A. HIPAA

The HIPAA Privacy, Security, and Breach Notification Rules (collectively, the HIPAA Rules) are widely known as providing a federal floor of privacy, security, and breach notification protections for PHI, ePHI, and uPHI, respectively.[69] Some background information is necessary to show why this is not always true, including why the HIPAA Rules do not protect the medical records that document postsecondary students' encounters with most university-owned student health centers.

1. The HIPAA Privacy Rule

President Clinton signed HIPAA into law on August 21, 1996.[70] Section 264 of HIPAA directed the Secretary of HHS to submit to Congress detailed

---

[66] *Infra* Parts I.A–B.

[67] *Infra* Parts I.A–B.

[68] *Infra* Part I.C.

[69] *See, e.g.*, *Frequently-Asked Question No. 399, Does the HIPAA Privacy Rule Preempt State Laws?*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html (last visited Feb. 5, 2023) ("The HIPAA Privacy Rule provides a Federal floor of privacy protections for individuals' individually identifiable health information where that information is held by a covered entity or by a business associate of the covered entity."); *Frequently-Asked Question No. 2000, Why Is the HIPAA Security Rule Needed and What Is the Purpose of the Security Standards*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/2000/why-is-hipaa-needed-and-what-is-the-purpose-of-security-standards/index.html (last visited Feb. 5, 2023) ("The Security Rule establishes a Federal floor of standards to ensure the availability, confidentiality and integrity of e-PHI.").

[70] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (Aug. 21, 1996); *President Signs Insurance Portability Bill Into Law*, WASH. POST. (Aug. 22, 1996),

recommendations regarding standards to protect the privacy of individually identifiable health information (IIHI).[71] According to HIPAA, these *recommendations* were to address (1) the legal rights that individuals should have with respect to their IIHI, (2) the procedures that should be developed for individuals to exercise their rights, and (3) the uses and disclosures of IIHI that should be authorized.[72] HHS's recommendations were due to Congress within one year of the date of enactment of HIPAA.[73] HHS responded in a timely manner, providing Congress with the guidance it needed to pass privacy legislation by September of 1997.[74]

The HIPAA statute explained that if Congress did not pass privacy legislation within three years of the date of the statute's enactment, the obligation to promulgate administrative regulations governing privacy would fall to HHS.[75] Congress missed its three-year deadline, so the responsibility to adopt privacy regulations fell to HHS. HHS again responded in a timely manner.[76] On November 3, 1999,[77] and December 28, 2000,[78] HHS issued a proposed and final privacy rule (HIPAA Privacy Rule). On March 27, 2002,[79] and August 14, 2002,[80] HHS issued proposed and final modifications to the HIPAA Privacy Rule. With the exception of technical corrections and conforming amendments, these rules as reconciled remained largely unchanged between 2002 and 2009.[81] On February 17, 2009, President Obama signed the

---

https://www.washingtonpost.com/archive/politics/1996/08/22/president-signs-insurance-portability-bill-into-law/46ea70fe-50ee-4c17-8209-3f99045b123e/.

[71] Health Insurance Portability and Accountability Act § 264(a).

[72] *Id.* § 264(b).

[73] *Id.* § 264(a).

[74] *Confidentiality of Individually Identifiable Health Information*, U.S. DEP'T OF HEALTH & HUM. SERVS., ASS'T SEC. PLANNING & EVAL. (Sept. 10, 1997), https://aspe.hhs.gov/reports/confidentiality-individually-identifiable-health-information (providing recommendations to Congress as required by § 264 of HIPAA).

[75] Health Insurance Portability and Accountability Act § 264(c)(1).

[76] *See infra* notes 77–78.

[77] Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918 (proposed Nov. 3, 1999) (to be codified at 45 C.F.R. pts. 160–64).

[78] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000).

[79] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14776 (proposed Mar. 27, 2002) (to be codified at 45 C.F.R. pts. 160, 164).

[80] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160, 164).

[81] *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, 66 Fed. Reg. 12434, 12434 (Feb. 26, 2001) (codified at 45 C.F.R. pts. 160, 164); Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information Published December 28, 2000, 65 Fed. Reg. 82944, 82944 (Dec. 29, 2000) (codified at 45 C.F.R. pts. 160, 164).

American Recovery and Reinvestment Act (ARRA) into law.[82] Division A, Title XIII of ARRA, better known as the Health Information Technology for Economic and Clinical Health Act (HITECH), required HHS (1) to expand the application of the HIPAA Privacy Rule, (2) to modify some of the use and disclosure requirements, and (3) to adopt new breach notification rules, among other changes.[83] HHS responded to HITECH's directives with proposed and final rules on July 14, 2010,[84] and January 25, 2013,[85] respectively.

As amended by HITECH, the HIPAA Privacy Rule regulates covered entities[86] and business associates[87] with respect to their uses and disclosures of a class of information known as PHI.[88] Covered entities include health plans,[89] health care clearinghouses,[90] and certain health care providers[91] (i.e., those health care providers that transmit health information in electronic form in connection with certain standard transactions).[92] Of relevance to this Article, health care providers are defined to include persons and organizations that furnish, bill, or get paid for "health care in the normal course of business."[93] "Health care" is defined to include "care, services, or supplies related to the health of an individual" (including "[p]reventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care") as well as the "[s]ale or dispensing of a drug, device, equipment, or other item in accordance with a prescription."[94]

---

[82] *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, §§ 13001–424, 123 Stat. 115, 226–79; Scott Horsley & Melissa Block, *Obama Signs Stimulus Bill*, NPR (Feb. 17, 2009), https://www.npr.org/2009/02/17/100785745/obama-signs-stimulus-bill.

[83] *See* 42 U.S.C. §§ 17932–39 (2012).

[84] *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40868 (proposed July 14, 2010) (to be codified at 45 C.F.R. pts. 160, 164).

[85] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5688 (Jan. 25, 2013) (codified at 45 C.F.R. pgs. 160, 164).

[86] 45 C.F.R. § 160.103 (defining covered entity); *id*. § 160.102(a) (applying the HIPAA Rules to covered entities)).

[87] *Id*. § 160.103 (defining business associate); *id*. § 160.102(b) (applying the HIPAA Rules to business associates).

[88] *Id*. § 160.103 (defining protected health information).

[89] *Id*. (defining health plan).

[90] *Id*. (defining health care clearinghouse).

[91] *Id*. (defining health care provider).

[92] *Id*. (defining covered entity).

[93] *Id*. (defining health care provider).

[94] *Id*. (defining health care).

University-owned student health centers typically provide a wide range of preventive, diagnostic, and therapeutic care services[95]—not only to students but many times to faculty, staff, and their dependents as well.[96] University pharmacies, which tend to be located adjacent to student health centers, sell and dispense prescription drugs.[97] As a result, both student health centers and

[95] *See, e.g.*, *Student Health and Wellness*, UNIV. CONN., https://studenthealth.uconn.edu/preventive-care/ (last visited Feb. 5, 2023) ("[University of Connecticut] Student Health and Wellness provides preventive care and health screening services to ensure our students are happy and healthy!"); *Student Health Clinic*, UNIV. OKLA. HEALTH SCI. CTR., https://students.ouhsc.edu/current-students/student-wellbeing/health-clinic (last visited Feb. 5, 2023) ("The OU Health Student Health Clinic provides acute and chronic care for injuries and illnesses, as well as routine preventative care.").

[96] *See, e.g.*, *Eligibility and Insurance*, HARV. UNIV. HEALTH SERVS., https://huhs.harvard.edu/eligibility-insurance#gsc.tab=0 (last visited Feb. 5, 2023) (stating that Harvard University faculty, staff, and their dependents may be seen at any of the three convenient Harvard University Health Services locations); *University Health Services*, PRINCETON UNIV., https://uhs.princeton.edu (last visited Feb. 5, 2023) ("We provide quality medical, health and wellness services to Princeton University undergraduate and graduate students, their dependents, and faculty and staff."); *Eligibility for Care*, UNIV. FLA. STUDENT HEALTH CARE CTR., https://shcc.ufl.edu/fees-and-insurance/university-shcc-fees/eligibility/ (last visited Feb. 5, 2023) (stating that students, spouses, and dependents are permitted to use the University of Florida Student Health Care Center); *University Health Center Services for UGA Faculty and Staff*, UNIV. HEALTH CTR. UNIV. GA., https://healthcenter.uga.edu/info/faculty-staff-info/ (last visited Feb. 5, 2023) (stating that University of Georgia University Health Center services are available to faculty and staff); *Who Can Use UHS?*, U. MICH. HEALTH SERV., https://uhs.umich.edu/who (last visited Feb. 5, 2023) (stating that University of Michigan students as well as current and former faculty and staff, visiting scholars, graduates, retirees, spouses, and other qualified adults and dependents may use the University of Michigan Health Service); *Frequently Asked Questions About Campus Health*, UNIV. N.C. CAMPUS HEALTH, https://campushealth.unc.edu/about-us/frequently-asked-questions-about-campus-health/ (last visited Feb. 5, 2023) (stating that all students, postdoctoral fellows, and spouses of undergraduate students, graduate students, and postdoctoral fellows can access care through the University of North Carolina Campus Health Center); *UT Austin Faculty/Staff*, UNIV. TEX. AUSTIN UNIV. HEALTH SERVS., https://healthyhorns.utexas.edu/facultyandstaff.html (last visited Feb. 5, 2023) (stating that the University of Texas University Health Services provides medical care to undergraduate, graduate, and professional students as well as faculty and staff); *Comprehensive Health Care on Campus*, UNIV. WASH., https://wellbeing.uw.edu/hall-health/about-hall-health/ (last visited Feb. 5, 2023) (stating that, "[The University of Washington] Hall Health Center is an outpatient clinic that provides health care to University of Washington students, alumni, faculty, and staff as well as the general community"); *Student Health Center*, UNIV. UTAH, https://studenthealth.utah.edu (last visited Feb. 5, 2023) (stating that the University of Utah Student Health Center "[p]rovid[es] quality healthcare to students, spouses, and their dependents").

[97] *See, e.g.*, *Pharmacy*, UNIV. HEALTH CTR. UNIV. GA., https://healthcenter.uga.edu/services/pharmacy/ (last visited Feb. 5, 2023) ("The goal of the Pharmacy is to provide efficient, professional, confidential, and economical prescription service to the students of the University of Georgia. Pharmacy services are now available to UGA faculty [and] staff, retired faculty [and] staff, and dependents."); *Pharmacy*, UC DAVIS STUDENT HEALTH & COUNSELING SERVS., https://shcs.ucdavis.edu/services/pharmacy (last visited Feb. 5, 2023) ("[Student Health and Counseling Services] Pharmacy is here to serve the college health needs for all registered students. We have a wide variety of prescription . . . medications."); *Student Health Center, Pharmacy*, TEX. STATE UNIV., https://www.healthcenter.txst.edu/rx.html (last visited Feb. 5, 2023) ("The Texas State Student Health Center has a fully licensed pharmacy on-site. The pharmacy is for students, faculty, staff and visitors to campus . . . . We offer medications at reasonable prices and our pharmacists will answer any questions you have.").

university pharmacies fall within the definition of a "health care provider"[98] and will be regulated by the HIPAA Privacy Rule with respect to their uses and disclosures of PHI if they transmit health information in electronic form in connection with a standard transaction.[99] The most common standard transaction is the health insurance claim transaction.[100] If a student health center or university pharmacy takes any form of insurance (public or private) and bills insurance electronically on behalf of even one patient (and not necessarily a patient who might later claim a HIPAA violation), the student health center and the university pharmacy will be HIPAA covered entities for all of their patients. Most student health centers and university pharmacies take several forms of insurance, including student health insurance, and bill those insurances electronically.[101] As a result, most student health centers and university pharmacies are HIPAA covered entities that must comply with the HIPAA Privacy Rule when using or disclosing PHI.[102]

Before using or disclosing PHI, the HIPAA Privacy Rule requires covered entities to adhere to technical permission rules depending on the purpose of the information use or disclosure (hereinafter Use and Disclosure Rules).[103] One Use and Disclosure Rule allows covered entities to use and disclose PHI without prior permission from the individual who is the subject of the PHI—but only in certain limited situations.[104] That is, covered entities may freely use and disclose PHI without any form of prior permission in order to carry out certain

---

98 *See supra* notes 93–94 (defining health care provider and health care).

99 45 C.F.R. § 160.103 (2022) (defining covered entity to include only those health care providers who "transmit[] any health information in electronic form in connection with a [standard] transaction").

100 *Id.* (defining transaction to include health care claims).

101 *See, e.g.*, *Pharmacy Billing and Insurance*, UNIV. HEALTH SERVS., https://health.uoregon.edu/pharmacybilling (last visited Feb. 5, 2023) (listing the forms of insurance accepted by the University of Oregon Pharmacy); *Pharmacy*, UNIV. HEALTH SERVS., https://healthcenter.olemiss.edu/pharmacy/ (last visited Feb. 5, 2023) ("We bill most insurance carriers for you."); *Pharmacy*, U. OKLA HEALTH SERVS., https://www.ou.edu/healthservices/medical-services/pharmacy (last visited Feb. 5, 2023) ("Our pharmacy accepts most prescription insurance plans.").

102 HIPAA covered entities also must comply with the HIPAA Security Rule with respect to their ePHI and the HIPAA Breach Notification Rule with respect to their uPHI. *See infra* Parts I.A.2–3.

103 *See* 45 C.F.R. §§ 164.502–.514 (setting forth the use and disclosure requirements applicable to covered entities and business associates).

104 *See id.*

treatment,[105] payment,[106] and health care operations (collectively, TPO)[107] activities,[108] as well as certain public benefit (PB) activities.[109] Although the TPO and PB disclosures that may be made pursuant to this first rule are not the focus of this Article, a second Use and Disclosure Rule—a default rule—requires covered entities to obtain the prior written authorization of any adult subjects of PHI before using or disclosing their PHI in situations that do not fall under the first rule.[110] Under this second rule, for example, a covered student health center may not disclose a law professor's cancer diagnosis to the law professor's parents, the law school dean, or the university president without the professor's prior written authorization.[111] A covered university pharmacy also may not sell a law school dean's prescription information to People Magazine unless the pharmacy obtains the prior written authorization of the dean and the authorization form states that the pharmacy will obtain remuneration in exchange for the information disclosure.[112] This second Use and Disclosure Rule is very important. It prevents unauthorized disclosures of adult treatment records to parents and third parties for activities unrelated to TPO and PB.[113]

In addition to these Use and Disclosure Rules, the HIPAA Privacy Rule also gives individuals five rights with respect to their PHI, including the right to: (1) receive a notice of privacy practices,[114] (2) request additional privacy

---

[105] *See, e.g., id.* §§ 164.502(a)(1)(ii), 164.506. Among other activities, treatment includes "the provision, coordination, or management of health care and related services by one or more health care providers." *Id*. § 164.501.

[106] *See, e.g., id.* §§ 164.502(a)(1)(ii), 164.506. Payment activities are "[t]he activities undertaken by . . . a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan" as well as the activities of "[a] health care provider or health plan to obtain or provide reimbursement for the provision of health care." *Id*. § 164.501.

[107] The HIPAA Privacy Rule defines "health care operations" with respect to a list of activities that are related to a covered entity's covered functions. *See id*. § 164.501. These activities include, but are not limited to, quality assessment and improvement, medical and other forms of health professional education, and legal services. *Id.* (defining "health care operations").

[108] *See id*. § 164.506(c)(1) (permitting "[a] covered entity [to] use or disclose [PHI] for its own treatment, payment, or health care operations"); *id*. § 164.506(c)(1)–(4) (permitting a covered entity to disclose PHI to certain recipients for the recipients' "treatment, payment, or health care operations" activities, respectively).

[109] *See, e.g., id*. § 164.512(k)(6). Covered entities may use and disclose PHI for twelve different public policy activities without the prior written authorization of the individual who is the subject of the information. *See id*. § 164.512(a)–(l).

[110] *See* 45 C.F.R. § 164.508(a)(1) (titled "Uses and disclosures for which an authorization is required"). *Compare* 34 C.F.R. § 99.31(a)(8) (2011) (allowing FERPA-regulated universities to disclose an adult student's education records to the student's parents without the student's consent if the student is a dependent of the parent under § 152 of the Internal Revenue Code), *with* 45 C.F.R. § 164.508(a)(1).

[111] *See* 45 C.F.R. § 164.508(a)(1).

[112] *See id*. § 164.508(a)(4).

[113] *See supra* note 110.

[114] 45 C.F.R. § 164.520.

protections,[115] (3) access PHI (including the right to receive a paper or electronic copy of PHI),[116] (4) request amendment of PHI,[117] and (5) receive an accounting of disclosures of PHI[118] (collectively, the Individual Rights). Pursuant to the right to request additional privacy protections, for example, a covered student health center must accommodate a law professor's request for lab test results to be sent to the professor's personal email rather than the professor's university email because the latter email account may be accessed by the professor's administrative assistant.[119] By further example, a law school dean has the right to have a student health center amend incorrect PHI that is contained in the dean's medical records.[120] If the dean's medical records state that the dean has given birth to two children when the dean has no children, the dean can have the incorrect record amended.[121] By final illustrative example, a law school director of admissions has the right to receive an accounting of the PHI disclosures made by the health center about the director, subject to several exceptions.[122] For example, if the health center discloses the director's medical records to the law school dean without the director's prior written authorization, the director has the right to be notified of that disclosure in an accounting.[123] Lastly, the HIPAA Privacy Rule contains a set of ten administrative requirements (hereinafter Administrative Requirements).[124] These Administrative Requirements include, but are not limited to, human resources requirements,[125] patient protection

115 *Id.* § 164.522.
116 *Id.* § 164.524.
117 *Id.* § 164.526.
118 *Id.* § 164.528.
119 *See id.* § 164.522(b)(1)(i).
120 *See id.* § 164.526(a)(1).
121 *See id.*
122 *See id.* § 164.528(a)(1).
123 *See id.*
124 *Id.* § 164.530(a)–(j).
125 The HIPAA Privacy Rule's human resources requirements include the requirement to designate privacy personnel who are responsible for receiving privacy-related complaints and the requirement to train workforce members on privacy policies and procedures. *Id.* § 164.530(a)–(b).

requirements,[126] post-violation requirements,[127] and paperwork and documentation requirements.[128]

For example, a covered student health center that discards non-shredded faculty medical records in a dumpster located behind the center would violate the patient protection requirement.[129] By further example, a law school faculty member who believes her privacy rights have been violated has a legal right to complain not only to the student health center but also to the Secretary of HHS.[130] The student health center has violated the human resources requirement and the patient protection requirement if the health center does not notify the faculty member of the right to complain (as well the right to be free from retaliation in exchange for complaining) in the health center's notice of privacy practices or if the health center does not provide an avenue for lodging and receiving such complaints.[131] By still further example, a covered student health center cannot intimidate, threaten, coerce, or discriminate against a law school dean who exercises the dean's rights under the Privacy Rule, including the right to complain to the Secretary of HHS.[132] By final illustrative example, a covered student health center that violates a law school dean's privacy must mitigate any harmful effects of that privacy violation pursuant to the post-violation requirements.[133]

---

[126] The HIPAA Privacy Rule's patient protection requirements include having in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information; not intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against any individual for the exercise by the individual of any right established under the HIPAA Privacy Rule; and not making an individual waive any rights under the HIPAA Privacy Rule as a condition of being treated or insured. *Id*. § 164.530(c), (g), (h).

[127] The HIPAA Privacy Rule's post-violation requirements include allowing individuals who believe their privacy rights have been violated to complain to the covered entity, sanctioning workforce members who violate the HIPAA Privacy Rule, and mitigating harmful effects of unauthorized information uses and disclosures. *Id.* § 164.530(d)–(f).

[128] The HIPAA Privacy Rule's paperwork and documentation requirements include the requirement to draft and implement privacy policies and procedures as well as the requirement to maintain such policies and procedures in written or electronic form. *Id*. § 164.530(i)–(j).

[129] *See id*. § 164.530(c)(1).

[130] *See id*. § 164.530(d) (authorizing complaints to the covered entity); *id*. § 160.306 (authorizing complaints to the Secretary of HHS).

[131] *See id*. § 164.520(b)(1)(vi).

[132] *See id*. § 164.530(g).

[133] *See id*. § 164.530(f).

2. The HIPAA Security Rule

In addition to the Use and Disclosure Rules, Individual Rights, and Administrative Requirements set forth in the HIPAA Privacy Rule, all of which apply to PHI, HHS also has promulgated a security rule (the HIPAA Security Rule) designed to protect ePHI.[134] In particular, the HIPAA Security Rule requires covered entities and business associates to implement three classes of safeguards—administrative, physical, and technical—to: (1) ensure the confidentiality, integrity, and availability of ePHI; (2) guard against reasonably anticipated threats or hazards to the security or integrity of such information; and (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.[135] ePHI is defined as individually identifiable health information that is transmitted by electronic media or maintained in electronic media.[136]

The first class of safeguards (the administrative safeguards) require covered entities to designate a security official responsible for the development and implementation of the covered entity's security policies and procedures.[137] These policies and procedures must: (1) prevent, detect, contain, and correct security violations; (2) ensure that workforce members have appropriate access to ePHI; (3) prevent workforce members who should not have access to ePHI from obtaining such access; (4) create a security awareness and training program for all workforce members; and (5) address and respond to security incidents, emergencies, environmental problems, and other occurrences such as fire, vandalism, system failure, and natural disaster that affect systems containing ePHI and the security of ePHI, among other requirements.[138] For example, the administrative safeguards would require a covered student health center to implement policies and procedures prohibiting student workers from accessing their professors' ePHI if the student workers do not need to access such ePHI to perform their job duties at the health center.[139]

The second class of safeguards (the physical safeguards) require covered entities to implement policies and procedures that: (1) limit physical access to electronic information systems and the facilities in which they are located; (2)

---

134 The HIPAA Security Rule, 45 C.F.R. §§ 164.302–.318. The HIPAA Security Rule implements § 262(a) of HIPAA. *See id.*; 42 U.S.C. § 1320d–2(d)(1).

135 45 C.F.R. § 164.306(a)(1)–(3).

136 *Id.* § 160.103 (defining ePHI).

137 *Id.* § 164.308.

138 *Id.*

139 *See id.*

address the safeguarding, functioning, and physical attributes of workstations through which ePHI is accessed; and (3) govern the receipt and removal of hardware and electronic media that contain ePHI.[140] For example, the physical safeguards would require a covered student health center to implement policies and procedures prohibiting university students who do not work in the health center from entering secure parts of the center and accessing faculty and staff members' ePHI.[141]

The third and final class of safeguards (the technical safeguards) require covered entities to implement: (1) technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights; (2) hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI; (3) policies and procedures to protect ePHI from improper alteration or destruction; (4) procedures to verify that a person or entity seeking access to ePHI is the one claimed; and (5) technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.[142] For example, the technical safeguards would require a covered student health center to record and examine activity in its electronic medical records system, including identifying any individual who is accessing such records without permission and/or without a need to know such information.[143]

3. The HIPAA Breach Notification Rule

In addition to its Privacy and Security Rules, which apply to PHI and ePHI, respectively, HHS also has promulgated a Breach Notification Rule that applies in the event of a breach of uPHI.[144] In particular, the HIPAA Breach Notification Rule requires covered entities, following the discovery of a breach[145] of uPHI,[146] to notify each individual whose uPHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of

---

[140] *Id.* § 164.310.

[141] *See id.*

[142] *Id.* § 164.312.

[143] *See id.*

[144] The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–.414. The HIPAA Breach Notification Rule implements § 13402 of HITECH. *See id.*; 42 U.S.C. § 17932.

[145] 45 C.F.R. § 164.402 (defining breach as the "acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the [PHI]" and providing exceptions to the definition of breach).

[146] *Id.* § 164.402 (defining uPHI as PHI that is "not rendered unusable, unreadable, or indecipherable to unauthorized persons" through the use of certain HHS-specified technologies or methodologies).

such breach.[147] The notification, which shall be provided without undue delay and within sixty calendar days after the discovery of the breach, must include: (1) a brief description of the nature of the breach, including the date of the breach and the date of its discovery; (2) a description of the types of uPHI involved in the breach; (3) any steps the individual should take to protect herself from potential harm resulting from the breach; (4) a brief description of the steps taken by the covered entity to investigate the breach, to mitigate harm to individuals whose uPHI was part of the breach, and to protect against future breaches; and (5) contact information sufficient to allow individuals to ask questions or learn additional information about the breach.[148]

When a breach involves the uPHI of more than 500 residents of a state or jurisdiction, the HIPAA Breach Notification Rule also requires the covered entity to notify prominent media outlets serving the state or jurisdiction.[149] When a breach involves the uPHI of 500 or more individuals, regardless of their state of residency, the covered entity must also notify the Secretary of HHS within sixty calendar days after the discovery of the breach.[150] Finally, when the breach involves the uPHI of less than 500 individuals, regardless of their state of residency, the covered entity must notify the Secretary of HHS not later than sixty calendar days after the end of the calendar year.[151]

To illustrate the application of the HIPAA Breach Notification Rule, assume a covered student health center fails to terminate a former employee's access to the health center's electronic medical records system and later discovers that the former employee continued to access unsecured faculty and staff medical records for unauthorized purposes. In this case, the health center would have an obligation to notify each faculty and staff member whose uPHI had been breached.[152] This notification is important. It allows faculty and staff members whose uPHI has been breached to take steps to protect themselves, such as freezing their credit[153] and demanding that the covered entity mitigate the harmful effects of privacy violations.[154]

---

147 *Id.* § 164.404(a)(1).

148 *Id.* § 164.404(b)–(c).

149 *Id.* § 164.406(a).

150 *Id.* § 164.408(b).

151 *Id.* § 164.408(c).

152 *See supra* text accompanying notes 146–47.

153 45 C.F.R. § 164.404(c)(1)(C) (requiring covered entities to notify individuals of the steps they can take to protect themselves from harm following a breach of their uPHI).

154 *Id.* § 164.530 (requiring covered entities to mitigate harmful effects of HIPAA Privacy Rule violations).

In addition, and depending on the number of faculty and staff persons whose uPHI had been breached, the student health center also must notify the Secretary of HHS either within sixty days of the breach (if 500 or more individuals are affected) or within sixty days of the end of the calendar year (if fewer than 500 individuals are affected).[155] And, if the breach involves the uPHI of 500 or more faculty or staff who are residents of the same state, the student health center must notify prominent media outlets of that state.[156] For example, if the University of Georgia (UGA) Health Center experiences a breach of the uPHI of more than 500 faculty and staff members who are residents of Georgia, then the Health Center must notify prominent media outlets serving Georgia of the breach.[157] But if the same breach also involves the uPHI of 30 UGA faculty and staff members who happen to reside in South Carolina, South Carlina media outlets would not need to be notified.[158]

4. HIPAA Rules Enforcement

Any person who believes a covered entity is not complying with the HIPAA Rules may complain to the Secretary of HHS.[159] If HHS receives a complaint about a covered entity, including a covered student health center or covered university pharmacy, HHS will investigate when a preliminary review of the facts indicates a possible HIPAA Privacy Rule violation due to willful neglect.[160] If HHS's investigation indicates noncompliance, the agency's resolution options include: (1) providing technical assistance to the covered student health center or pharmacy; (2) obtaining voluntary compliance by the health center or pharmacy; (3) entering into a settlement agreement that requires the health center or pharmacy to make a settlement payment to HHS; (4) requiring the health center or pharmacy to take corrective action pursuant to a corrective action plan (CAP); (5) imposing civil monetary penalties on the health center or pharmacy; and/or (6) referring personnel at the health center or pharmacy to the federal Department of Justice (DOJ) for criminal penalties.[161] In 2022, civil

---

155 *See supra* text accompanying notes 149–51.

156 *See supra* text accompanying note 150.

157 *See supra* text accompanying note 150.

158 *See supra* text accompanying note 150.

159 45 C.F.R. § 160.306 (2022) (authorizing complaints to the Secretary of HHS); *see also id.* § 164.530(d) (authorizing complaints to the covered entity); *id.* § 164.520(b)(1)(vi) ("The notice [of privacy practices] must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.").

160 *Id.* § 160.306(c)(1).

161 *See id.* § 160.312.

monetary penalties applicable to HIPAA Rules violations ranged from: (1) $127 to $31,987 (for covered entities that did not know, and by exercising reasonable diligence would not have known, that the HIPAA Rules were violated); (2) $1,280 to $63,973 (for covered entities whose violations stemmed from reasonable cause but not willful neglect); (3) $12,794 to $63,973 (for covered entities whose violations occurred as a result of willful neglect but are remedied within thirty days); and (4) $63,973 to $63,973 (for covered entities whose violations occurred as a result of willful neglect and that are not remedied in a timely manner).[162] Regulations soon may be promulgated that would allow patients to share in civil monetary penalties imposed by HHS.[163]

Criminal penalties currently range from: (1) $50,000, one year in prison, or both (for covered entities who knowingly obtain or disclose individually identifiable health information in violation of the HIPAA Rules); (2) $100,000, five years in prison, or both (for covered entities whose wrongful conduct involves false pretenses); and (3) $250,000, ten years in prison, or both (for covered entities whose wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm).[164] If the federal government declines to exercise its HIPAA enforcement authority, the relevant state attorney general is permitted to bring a civil action against the clinic enjoining further HIPAA Rules violations, obtaining civil damages on behalf of the student, and seeking reimbursement for legal costs.[165]

In summary, the HIPAA Rules are widely known as providing a federal floor of privacy, security, and breach notification protections for individually identifiable health information.[166] As discussed above, the HIPAA Rules *do* provide a federal floor of privacy, security, and breach notification protections for the individually identifiable medical records of faculty, staff, dependents, and other non-student personnel who are permitted to obtain care or

---

[162] 42 U.S.C. § 1320d-5 (2022) (setting forth civil penalties applicable to HIPAA Privacy Rule violations); Annual Civil Monetary Penalties Inflation Adjustment, 87 Fed. Reg. 15100, 15109 (Mar. 17, 2022) (to be codified at 45 CFR 102) (updating these penalties for calendar year 2022 based on inflation).

[163] U.S. Dep't of Health & Hum. Servs., Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, 87 Fed. Reg. 19833, 19838 (Apr. 6, 2022) (to be codified at 45 CFR 164) (soliciting public comment on the distribution of civil penalties and monetary settlements to individuals harmed by HIPAA Privacy violations).

[164] 42 U.S.C. § 1320d-6 (2002) (setting forth criminal penalties applicable to HIPAA Privacy Rule violations).

[165] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13410(e), Stat. 226, 271–74 (2009); 42 U.S.C. § 1320d-5(5), (7) (2022).

[166] *See supra* note 69.

prescriptions at a covered student health center or university pharmacy.[167] As discussed in more detail below, however, the HIPAA Rules do *not* protect the medical and pharmacy records of postsecondary students who obtain care or prescriptions from student health centers and university pharmacies.[168]

5. Exception for Student Treatment Records

Recall that the HIPAA Privacy Rule only regulates covered entities with respect to their use and disclosure of a class of information known as PHI.[169] Further recall that the HIPAA Security Rule only regulates covered entities with respect to a class of information known as ePHI.[170] Finally, recall that the HIPAA Breach Notification Rule only requires individual, governmental, and media notification in the event of a breach of unsecured uPHI.[171] In order for any of the HIPAA Rules to apply, then, there must be PHI.

The HIPAA Rules generally define PHI as individually identifiable health information (IIHI);[172] that is, information that: (1) "[i]s created or received by a health care provider, health plan, employer, or health care clearinghouse"; and (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and that either (i) "identifies the individual"; or (ii) "[w]ith respect to which there is a

---

[167] *See, e.g.*, *Frequently Asked Question No. 518, Does FERPA or HIPAA Apply to Records on Students at Health Clinics Run by Postsecondary Institutions?*, U.S. DEP'T OF HEALTH & HUM. SERVS. [hereinafter HIPAA FAQ 518], https://www.hhs.gov/hipaa/for-professionals/faq/518/does-ferpa-or-hipaa-apply-to-records-on-students-at-health-clinics/index.html (last visited Feb. 5, 2023) (stating, "if the institution is a *HIPAA* covered entity and provides health care to *non*students, the individually identifiable health information of the clinic's *non*student patients is subject to the *HIPAA* Privacy Rule"; further stating, "[t]hus, for example, postsecondary institutions that are subject to both *HIPAA* and *FERPA* and that operate clinics open to staff, or the public, or both (including family members of students) are required to comply with . . . the *HIPAA* Privacy Rule with respect to the health records of their *non*student patients"); *supra* note 96 (providing illustrative examples of student health centers that provide services to non-students, including faculty, staff, and dependents).

[168] *See infra* Part I.A.5.

[169] *See, e.g.*, 45 C.F.R. § 164.500(a) (emphasis added) ("Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to *protected health information*.").

[170] *See, e.g.*, *id.* § 164.302 (emphasis added) ("A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic *protected health information* of a covered entity.").

[171] *See, e.g.*, *id.* § 164.404(a) (emphasis added) ("A covered entity shall, following the discovery of a breach of unsecured *protected health information*, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.").

[172] *Id.* § 160.103 (defining protected health information).

reasonable basis to believe the information can be used to identify the individual."[173] Because the medical and pharmacy records of postsecondary students who receive health care and prescriptions at student health centers and university pharmacies are created or received by health care providers, relate to a student's past or present physical or mental health condition or treatment therefore, and identify the student, the medical and pharmacy records fall within the definition of IIHI.[174]

The catch is that the HIPAA Rules except four types of IIHI from the definition of PHI, and two of these exceptions are education records and student treatment records.[175] Because the medical and pharmacy records that document the health care and prescriptions received by postsecondary students at student health centers and university pharmacies either fall into the definition of an education record or a student treatment record, the result is that not one of the HIPAA Rules protect them.[176] An understanding of how FERPA defines education records and student treatment records is necessary before proceeding.

B. FERPA

President Ford signed FERPA into law on August 21, 1974.[177] Enacted pursuant to Congress' spending power, FERPA applies to any public or private elementary, secondary, or postsecondary school and any state or local education agency that receives federal funds under a program administered by the U.S. Department of Education (DOE).[178] FERPA conditions federal education

---

[173] *Id*. (defining individually identifiable health information).

[174] *See id*.

[175] *Id*. (defining protected health information and excluding from that definition education records and student treatment records).

[176] The FTC also has promulgated a health-related breach notification rule that is similar to the HIPAA Breach Notification Rule in that it requires notification of data subjects as well as the federal government (in particular the FTC) in the event of certain breaches. *See* 16 C.F.R. § 318.3(a) (2023) (requiring each vendor of personal health records [PHRs], following the discovery of a breach of security of unsecured PHR identifiable health information [IHI] that is in a PHR maintained or offered by such vendor, to notify each individual who is a citizen or resident of the U.S. whose unsecured PHR IHI was acquired by an unauthorized person as a result of the breach as well as the FTC). The FTC breach notification rule does not apply to HIPAA covered entities, however. *Id*. § 318.1(a) ("It does not apply to HIPAA-covered entities . . . ."). Because most student health centers take insurance and bill insurance electronically (and thus fall into the definition of a covered entity), postsecondary students who are treated at student health centers would not benefit from FTC breach notification. *See supra* text accompanying notes 95–102 (explaining that most student health centers are HIPAA-covered entities).

[177] Family Educational Rights and Privacy Act, Pub. L. No. 93-380, 88 Stat. 484 (Aug. 21, 1974); U.S. DEP'T OF EDUC., LEGISLATIVE HISTORY OF MAJOR FERPA PROVISIONS 1 (June 2002), http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpaleghistory.pdf.

[178] 34 C.F.R. § 99.1(a) (2023).

funding on an educational agency or institution's ability to give a parent or eligible student[179] three limited rights, including (1) the opportunity to inspect and review the student's education records;[180] (2) the right to request an amendment of inaccurate or misleading education records;[181] and (3) the right to give prior written consent before personally identifiable information (PII)[182] from the student's education records is disclosed[183] (except in the dozen-plus situations in which consent is not required before a disclosure may occur).[184] These three FERPA rights are nowhere near as comprehensive as the rights set forth in the Use and Disclosure Rules, the Individual Rights, or the Administrative Requirements within the HIPAA Privacy Rule or the protections set forth in the HIPAA Security and Breach Notification Rules.[185]

In addition, many of the exceptions to consent under FERPA are not allowed under HIPAA.[186] For example, FERPA allows an educational institution (without the prior written consent of the student) to: (1) disclose PII from an eligible student's education records to the student's parents if the student is claimed as a dependent for tax purposes under the Internal Revenue Code; (2) inform parents of students under the age of twenty-one that the student has violated any law or policy concerning the use or possession of alcohol or a controlled substance if the institution determines that the student committed a disciplinary violation with respect to that use or possession; and (3) share information with a parent that is based on a university official's personal knowledge or observation and that is not based on information contained in an education record.[187] HIPAA, on the other hand, would require a patient's prior written authorization before a covered health care provider could: (1) disclose

---

[179] An eligible student is defined as a "student who has reached 18 years of age or is attending an institution of postsecondary education." *Id.* § 99.3 (2023) (defining eligible students). When a student becomes an eligible student, the rights accorded to, and consent required of, parents under FERPA transfer from the parents to the student. *Id.* § 99.5(a)(1).

[180] *Id.* §§ 99.10–.12 .

[181] *Id.* §§ 99.20–.22.

[182] PII includes, but is not limited to, a student's name, address, social security number, student number, biometric record, date of birth, place of birth, mother's maiden name, and "[o]ther information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty." *Id.* § 99.3 (defining PII).

[183] *Id.* § 99.30(a).

[184] *Id.* § 99.31(a).

[185] *Compare* Parts I.A.1–3 (codifying dozens of comprehensive rights available under the HIPAA Privacy, Security, and Breach Notification Rules), *with supra* text accompanying notes 181–83 (listing three discrete rights available under FERPA).

[186] *See infra* note 188.

[187] *See* 34 C.F.R. § 99.31(a) (listing these and other exceptions to consent).

an adult patient's PHI to the patient's parents, even if the patient is claimed as a dependent for tax purposes under the Internal Revenue Code; (2) inform parents of patients over the age of eighteen but under the age of twenty-one that the patient has violated any law or policy concerning the use or possession of alcohol or a controlled substance; or (3) share information about an adult patient with the patient's parents even if that information is based on the provider's personal knowledge or observation and is not based on information contained in the patient's medical record.[188]

Most importantly, however, the three FERPA rights only apply to "education records."[189] FERPA broadly defines "education records" as records that directly relate to a student and that are maintained by the educational agency or institution.[190] At first glance, it would appear that a postsecondary student's medical and pharmacy records would meet this definition. After all, medical and pharmacy records relate to a student and are maintained by a university-owned health center or pharmacy. However, FERPA excludes from the definition of education records certain student treatment records, defined as:

> records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.[191]

---

188 *Compare id.* (listing several exceptions to consent under FERPA), *with* 45 C.F.R. §§ 164.506, 164.512 (listing the exceptions to patient authorization under the HIPAA Privacy Rule, none of which apply to the scenarios described in the text accompanying footnote 187).

189 *See supra* text accompanying notes 180–81, 183.

190 34 C.F.R. § 99.3 (defining education record).

191 20 U.S.C. § 1232g(a)(4)(A)(B)(iv). The regulations implementing FERPA provide a slightly different definition; that is, "[r]ecords on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are: (i) Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity; (ii) Made, maintained, or used only in connection with treatment of the student; and (iii) Disclosed only to individuals providing the treatment. For the purpose of this definition, 'treatment' does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution." 34 C.F.R. § 99.3 (2023) (excluding student treatment records from the definition of education record and defining student treatment records).

HHS provides examples of records that meet this definition, including "health or medical records that a university psychologist maintains only in connection with the provision of treatment to an eligible student" as well as "health or medical records that the campus health center or clinic maintains only in connection with the provision of treatment to an eligible student."[192]

Because student treatment records are excluded from the definition of education records under FERPA, postsecondary students do not have FERPA-related rights with respect to them. For example, postsecondary students do not have the right under FERPA to inspect and review their student treatment records or the right to request an amendment of student treatment records that may be inaccurate or misleading.[193] As discussed above, postsecondary students also do not benefit from any of the comprehensive legal rights set forth in the HIPAA Privacy, Security, and Breach Notification Rules because student treatment records are excluded from the definition of PHI under the HIPAA Rules.[194]

One curious clause within the definition of student treatment records provides that such records must not be "available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice."[195] HHS and DOE interpret this clause to mean that a student health center or university pharmacy can disclose student treatment records—without the student's prior written consent—to other treatment providers, including treatment providers that are not affiliated with the university as well as treatment providers that are selected by the student.[196]

When copies of student treatment records are disclosed to these other treatment providers for treatment purposes, the *original* records (i.e., those records still in the hands of the student health center or university pharmacy) do not lose their status as student treatment records and, thus, remain excluded from

---

192 HIPAA FAQ 518, *supra note* 167.

193 *See supra* notes 180–81.

194 *See supra* Part I.A.

195 20 U.S.C. § 1232g(a)(4)(A)(B)(iv).

196 U.S. DEP'T OF HEALTH & HUM. SERVS. & U.S. DEP'T EDUC., JOINT GUIDANCE ON THE APPLICATION OF FERPA AND HIPAA TO STUDENT RECORDS 5 (updated 2019) [hereinafter HHS & DOE JOINT GUIDANCE] ("An educational agency or institution may only disclose an eligible student's treatment records to individuals who are providing treatment to the student (including health care professionals who are not part of, nor acting on behalf of, the educational agency or institution (*e.g.*, third-party health care providers)), and a physician or other appropriate professional of the student's choice.").

protection under both HIPAA and FERPA.[197] That is, the original records in the hands of the student health center or university pharmacy are only protected by state law.[198] The *disclosed* medical record copies could become protected by the HIPAA Rules, however, if they are sent to a non-university affiliated HIPAA-covered health care provider (i.e., a health care provider who takes insurance and bills insurance electronically).[199] The *disclosed* medical record copies could also remain protected only by state law if they are sent to a non-HIPAA-covered health care provider (i.e., a health care provider who does not take insurance and therefore does not bill insurance electronically).[200]

A hypothetical involving the University of Texas Health Services in Austin, Texas[201] may be used to illustrate these rules. Assume the University of Texas Health Services discloses a student's treatment record to a physician in private practice in Houston to enable the student, who is from Houston, to receive follow-up care during the winter break, when the student will be visiting family in Houston. If the Houston physician is a HIPAA covered entity (i.e., the Houston physician takes insurance and bills insurance electronically), the Houston physician will be regulated by the HIPAA Rules and must protect the disclosed medical record copy in accordance with those Rules. If the Houston physician has a cash-only medical practice, however, the Houston physician will be regulated only by the limited privacy provisions set forth in state law, such as the Texas Medical Practice Act[202] and the Texas Medical Records Privacy Act.[203] Notably, the Texas Medical Records Privacy Act protects neither education records nor student treatment records.[204]

---

197 *See id*.

198 Part I.C. finds that state laws provide modest, if any, privacy, security, and breach notification protections for student treatment records. For more discussion, *see infra* Parts I.C.1–7.

199 *See supra* text accompanying notes 91–92 (explaining which health care providers are covered health care providers regulated by the HIPAA Privacy Rule); HHS & DOE JOINT GUIDANCE, *supra* note 196, at 18 ("[I]f the treatment records are disclosed to a third-party health care provider that is a HIPAA covered entity, the records would become subject to the HIPAA Privacy Rule.").

200 *See* HHS & DOE JOINT GUIDANCE, *supra* note 196.

201 UNIV. TEX. AUSTIN UNIV. HEALTH SERVS., https://www.healthyhorns.utexas.edu (last visited Feb. 5, 2023) ("University Health Services provides medical care to undergraduate, graduate and professional students as well as public health leadership at The University of Texas at Austin.").

202 *See* TEX. OCC. CODE ANN. §§ 159.001–.006 (West 2001) (Texas Medical Practice Act provisions governing the confidentiality of physicians' medical records).

203 *See* TEX. HEALTH & SAFETY CODE ANN. §§ 181.001(b)(2)(B), 181.004 (West 2015) (Texas Medical Records Privacy Act provisions that regulate non-HIPAA covered entities who come into possession of protected health information).

204 *See infra* text accompanying note 254.

The discussion above applies when a student health center discloses a student treatment record to a health care provider for treatment purposes. When a student health center discloses a student treatment record to a non-health care provider, either pursuant to the student's prior written consent[205] or pursuant to one of the dozen-plus exceptions to consent[206] set forth in FERPA, the now-disclosed records lose their status as student treatment records and revert back to education records protected by FERPA.[207] The result is that the student will have two very limited rights under FERPA,[208] including the right to inspect and review these education records[209] as well as the right to request amendment of incorrect and misleading education records.[210] However, the student will not have any of the significant privacy, security, or breach notification rights set forth in the HIPAA Rules because education records (and not just student treatment records) are

[205] *See* 34 C.F.R. § 99.30(a) (2023).

[206] Illustrative exceptions to consent allow a university to: (1) disclose PII from an eligible student's education records to the student's parents if the student is claimed as a dependent for tax purposes under the Internal Revenue Code; (2) disclose PII from an eligible student's education records to the student's parents in connection with a health or safety emergency if the parents' knowledge of the records is necessary to protect the health or safety of the student or other persons; (3) inform parents of students under the age of twenty-one that the student has violated any law or policy concerning the use or possession of alcohol or a controlled substance if the institution determines that the student committed a disciplinary violation with respect to that use or possession; and (4) share information with a parent that is based on a university official's personal knowledge or observation and that is not based on information contained in an education record. *See id*. § 99.31(a) (listing these and other exceptions to consent); HIPAA FAQ 518, *supra* note 167 (explaining that a FERPA-regulated school may disclose an eligible student's treatment records for purposes other than the student's treatment provided that the records are disclosed under one of the exceptions to written consent under 34 CFR § 99.31(a) or with the student's written consent under 34 CFR § 99.30). *See generally* Lynn M. Daggett, *The Myth of Student Medical Privacy*, 14 HARV. L. & POL'Y REV. 467 (2020) (examining FERPA exception-to-consent provisions that seemingly permit schools to access campus medical records of both student accusers and accused students in sexual misconduct matters and disclose them to college disciplinary panels and the other party); Lynn M. Daggett, *Female Student Patient "Privacy" at Campus Health Clinics: Realities and Consequences*, 50 U. BALT. L. REV. 77, 80 (2020) (arguing that "FERPA's 'cheesecloth' protection of student patient privacy [resulting from exception-to-consent provisions in FERPA] is unfair to all students, but it uniquely burdens female student patients at campus health clinics").

[207] *See generally* Iliana L. Peters, *Discovering "Medical Records" under Federal and State Law*, 12 J. HEALTH & LIFE SCI. L. 71, 80–81 (2019) (explaining when student treatment records revert back to education records protected by FERPA); Viola S. Lordi, *Ferpa—The Buckley Amendment: Safeguarding the Rights and Privacy of Parents and Students from Pre-School to Graduate and Professional School*, N.J. LAW., Dec. 2013, at 51, 52 ("In the event an eligible student's treatment records are utilized for any purpose other than the treatment of the eligible student, or become available to anyone other than the individuals providing the treatment, those records will be covered by the FERPA.").

[208] *See* HIPAA FAQ 518, *supra* note 167 ("If a school discloses an eligible student's treatment records for purposes other than treatment, the treatment records are no longer excluded from the definition of 'education records' and are subject to all other FERPA requirements, including the right of the eligible student to inspect and review the records.").

[209] 34 C.F.R. §§ 99.10–.12 (2023).

[210] *Id.* §§ 99.20–.22.

excluded from the definition of PHI under HIPAA.[211] Thus, the student will not have the right to request additional privacy protections[212] or the right to receive an accounting of disclosures,[213] both of which are afforded by the HIPAA Privacy Rule.[214] The student also will not benefit from the Use and Disclosure Rules or the Administrative Requirements set forth in the HIPAA Privacy Rule,[215] the administrative, physical, and technical safeguards set forth in the HIPAA Security Rule,[216] or the right to be notified of a privacy or security breach under the HIPAA Breach Notification Rule.[217] Because most students' treatment records are not disclosed for non-treatment purposes, most student treatment records do not revert into education records protected by FERPA. Instead, most student treatment records remain protected only by state law.[218]

In the preamble to the final HIPAA Privacy Rule, HHS explained its distaste for this confusing approach (i.e., the protection of student treatment records only under state law and the application of FERPA's limited protections to student-treatment-records-turned-education records) but felt hamstrung by the terms of the HIPAA statute, which did not specifically mention amending or preempting FERPA:

> While we strongly believe every individual should have the same level of privacy protection for his/her individually identifiable health information, Congress did not provide us with authority to disturb the scheme it had devised for records maintained by educational institutions and agencies under FERPA. We do not believe Congress intended to amend or preempt FERPA when it enacted HIPAA.[219]

HHS further explained that it considered requiring covered student health centers to protect student treatment records in accordance with the HIPAA Rules up until the records were disclosed for purposes other than treatment, at which point the records would become protected by FERPA and relieved of protection

---

211 *See* 45 C.F.R. § 160.103 (excluding education records protected by FERPA from the definition of protected health information protected by HIPAA).

212 *See* 45 C.F.R. § 164.522.

213 *See id.* § 164.528.

214 *See supra* text accompanying notes 114–23 (discussing these and other Individual Rights).

215 *See supra* text accompanying notes 124–32 (discussing these and other Administrative Requirements).

216 *See supra* Part I.A.2 (discussing these administrative, physical, and technical safeguards).

217 *See supra* Part I.A.3 (discussing the right to be notified of a breach of unsecured protected health information).

218 *See* text accompanying *supra* notes 205–11 (explaining this result).

219 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82483 (Dec. 28, 2000).

under HIPAA.[220] However, HHS chose "not to adopt this approach because it would be unduly burdensome to require providers to comply with two different, yet similar, sets of regulations and inconsistent with the policy in FERPA that these records be exempt from regulation to the extent the records were used only to treat the student."[221] For reasons explained in Parts II and III, this Article disagrees with HHS's decision.

C. State Law

Because most students treatment records are not disclosed for non-treatment purposes (either pursuant to consent or pursuant to an exception to consent), most student treatment records do not revert into education records protected by FERPA.[222] Instead, most student treatment records remain protected only by state law.[223] States have a variety of laws that establish potentially applicable privacy, security, and/or breach notification protections.[224] These state laws include professional practice acts, facility licensing laws, medical record privacy laws, data security laws, data breach notification laws, and consumer data protection laws.[225] Each of these laws will be discussed in turn.

1. State Professional Practice Acts

Most student health centers are staffed by some combination of physicians, physician assistants, and/or nurses practitioners.[226] Some (but not all) state professional practice acts that govern these health professionals establish requirements relating to confidentiality, although these requirements tend to be described in antiquated (e.g., "professional secret") or vague (e.g., "trust") terms that provide little guidance.[227] For example, the Oklahoma Medical Practice Act

---

220 *Id.*

221 *Id.*

222 *See* text accompanying *supra* notes 205–11 (explaining this result).

223 *See* text accompanying *supra* notes 205–11.

224 *See* Parts I.C.1–6.

225 *See* Parts I.C.1–6.

226 *See, e.g.*, *Clinical Staff*, UNIV. MIAMI STUDENT HEALTH SERV., https://studenthealth.studentaffairs.miami.edu/clinical-services/clinical-staff/index.html (last visited Feb. 5, 2023) (listing the physicians, physician assistants, and nurse practitioners who staff the Student Health Service at the University of Miami); *Meet the Staff*, UNIV. N. TEX DIV. STUDENT AFFS., https://studentaffairs.unt.edu/student-health-and-wellness-center/about/staff (last visited Feb. 5, 2023) (listing the physicians, physician assistants, and nurse practitioners who staff the Student Health and Wellness Center at the University of North Texas).

227 *See* Stacey A. Tovino, *Health Privacy, Security, and Information Management*, *in* LAWS OF MEDICINE: CORE LEGAL ASPECTS FOR THE HEALTH CARE PROFESSIONAL 223, 224–25 (Amirala S. Pasha ed., 2022).

authorizes the discipline of a physician who "[w]illfully betrays a professional secret to the detriment of the patient."[228] Similarly, the Nevada Medical Practice Act authorizes the discipline of a physician who "engages in conduct that violates the trust of a patient."[229] Likewise, the U.S. Virgin Islands Physician Assistant Licensing Act authorizes the discipline of a physician assistant who "except as required by law, violates patient confidentiality."[230] By final illustrative example, the Illinois Nurse Practice Act authorizes the discipline of a nurse practitioner who "[w]illfully or negligently violates the confidentiality" between nurse and patient.[231]

In addition to professional practice act provisions that refer to "secrets," "trust," and "confidentiality,"[232] some state professional practice acts also contain general, or catch-all, provisions that authorize discipline when the professional "brings disrepute to the profession," "undermines confidence in the profession," or "violates ethical principles."[233] For example, the Nevada Medical Practice Act allows the discipline of physicians who "engag[e] in conduct that brings the medical profession into disrepute."[234] Similarly, the Iowa Medical Practice Act allows the discipline of physicians who engage in "unethical or unprofessional conduct," including "a violation of the standards and principles of medical ethics."[235] Both types of provisions—those that specifically reference "secrets," "trust," or "confidentiality" as well as those that are more general—have been implicated in disciplinary cases involving allegations of privacy and confidentiality wrongdoing by a health care professional.[236]

---

228 OKLA. STAT. ANN. tit. 59, § 509(3) (2022).

229 NEV. REV. STAT. ANN. § 630.301(7) (West 2011).

230 V.I. CODE ANN. tit. 27 § 50n(9) (2022).

231 225 ILL. COMP. STAT. ANN. § 65/70-5(b)(36) (West 2022).

232 *See supra* notes 227–31.

233 *See infra* notes 234–36.

234 NEV. REV. STAT. ANN. § 630.301(9) (West 2011).

235 IOWA ADMIN. CODE R. § 653-23.1(4) (272C).

236 *See, e.g.*, Wassef, Case No. 02-2018-400 5 (Iowa Bd. Medicine March 25, 2022) (Amended Statement of Charges) (finding probable cause to charge an Iowa-licensed physician with violating an Iowa Medical Practice Act provision specifically requiring "[a] physician [to] maintain the confidentiality of all patient information obtained in the practice of medicine"); Sugarman v. Bd. of Registration in Med., 422 Mass. 338 (Sup. Jud. Ct. Mass., Suffolk, 1996) (disciplining a Massachusetts-licensed physician who, without prior authorization, disclosed a patient's medical record to a *Boston Globe* reporter; finding that the physician violated a catch-all Massachusetts Medical Practice Act provision prohibiting "conduct [that undermines] public confidence in the integrity of the medical profession"; and affirming a temporary order suspending the physician's license to practice medicine, imposing a $10,000 fine, and requiring the physician to complete one hundred hours of community service) (alteration in original).

That said, the substantive obligations of health professionals under state professional practice acts pale in comparison to the privacy, security, and breach notification obligations of HIPAA covered entities under federal law.[237] For example, state professional practice acts typically do not contain detailed Use and Disclosure Rules any Individual Rights,[238] or any Administrative Requirements[239] like those set forth in the HIPAA Privacy Rule. State professional practice acts also typically fail to establish security and breach notification requirements like those set forth in the HIPAA Security and Breach Notification Rules.[240]

Physicians, physician assistants, and nurse practitioners who fail to comply with the limited privacy obligations set forth in their professional practice acts do risk disciplinary action, including private reprimand, public censure, probation, community service, completion of additional clinical or ethics education, license suspension, license revocation, and/or fines payable to the licensing board.[241] The precise type and amount of discipline depends on the state in which the healthcare professional practices as well as the class of healthcare professional involved.[242] That said, state disciplinary measures pale in comparison to the civil and criminal penalties that apply to HIPAA Rules violations.[243] For example, Oklahoma physicians are subject to a maximum fine of only $5,000 per violation of the Oklahoma Medical Practice Act[244] and Illinois nurses are subject to a maximum fine of only $10,000 per violation of the Illinois Nurse Practice Act.[245] The HIPAA Rules, on the other hand, authorize civil penalties as high as $1,919,173[246] and criminal penalties as high as $250,000 combined with ten years imprisonment.[247] While most physicians and other health care professionals might be able to afford to violate confidentiality provisions set forth in practice acts, they likely cannot afford,

---

237 *Compare supra* text accompanying notes 228–33, *with supra* text accompanying Parts I.A.1–3.

238 *Compare supra* text accompanying notes 228–33, *with supra* text accompanying notes 114–23.

239 *Compare supra* text accompanying notes 228–33, *with supra* text accompanying notes 124–34.

240 *Compare supra* text accompanying notes 228–33, *with supra* Parts I.A.2–3.

241 *See, e.g.*, TEX. OCC. CODE ANN. § 164.001 (Vernon 2022) (referencing a wide variety of disciplinary actions available for Texas-licensed physicians who violate the Texas Medical Practice Act); *supra* note 236 (referencing two cases in which physicians who violated confidentiality were disciplined by their state medical boards).

242 *See infra* text accompanying notes 242–45 (referencing illustrative disciplinary measures applicable to different classes of health professionals in different states).

243 *Compare infra* text accompanying notes 244–45, *with infra* text accompanying notes 246–47.

244 OKLA. STAT. ANN. tit. 59, § 509.1(A)(9) (2022).

245 225 ILL. COMP. STAT. ANN. 65/70-5(a) (West 2022).

246 *See supra* text accompanying note 165.

247 *See supra* text accompanying note 167.

either financially, practically, or professionally, the civil and criminal penalties that attach to HIPAA Rules violations.

2. State Facility Licensing Laws

In addition to state professional practice acts, all states have facility licensing laws that regulate some, but not all, health care facilities.[248] Health care facilities subject to state licensing laws tend to include some combination of (in alphabetical order) abortion facilities, ambulatory surgery centers, assisted living facilities, birthing centers, community mental health centers, comprehensive outpatient rehabilitation facilities, end stage renal disease facilities, freestanding emergency medical care facilities, home health agencies, hospices, hospitals, laboratories, narcotic treatment programs, nursing homes, and rural health clinics.[249] Although the licensing laws governing these health care facilities do contain general privacy and confidentiality requirements,[250] most states do not have licensing laws applicable to university-owned student health centers.[251] Only the health care professionals who work in student health centers are licensed and regulated.[252] Thus, state facility licensing law is not a source of privacy protections for student treatment records.

3. State Medical Record Privacy Laws

Some states have medical records privacy laws that (in theory) apply to any medical record, regardless of the type of health care professional who has authored the record or the type of health care facility that maintains the record.[253] Many of these state medical record privacy laws have the laudable goal of extending HIPAA-like privacy protections to patients who are cared for by non-

---

[248] *See, e.g.*, *Health Care Facilities Regulation*, TEX. HEALTH & HUM. SERVS., https://www.hhs.texas.gov/providers/health-care-facilities-regulation (last visited Feb. 5, 2023) (listing some of these health care facilities as requiring a license to do business in Texas); *Licensing a Health Facility*, N. MEX. DEP'T OF HEALTH, https://www.nmhealth.org/about/dhi/hflc/prop/stli/ (last visited Feb. 5, 2023) (listing some of these health care facilities as requiring a license to do business in New Mexico).

[249] *See, e.g.*, *supra* note 246.

[250] *See generally* Tovino, *supra* note 227, at 226–28 (discussing the confidentiality requirements set forth in state health care facility licensing laws).

[251] *See* RICHARD T. YARMEL & EDWARD H. TOWNSEND, REGULATORY ISSUES FACING STUDENT HEALTH CENTERS 5, 7–8 (Aug. 2, 2016) (noting that student health centers are not regulated like hospitals and other traditional health care facilities; further noting that only the health care professionals who work in student health centers are regulated through their professional practice acts).

[252] *Id.*; *see supra* text accompanying notes 226–45 (summarizing the privacy and confidentiality obligations of health care professionals who work in student health centers).

[253] *See, e.g.*, Texas Medical Records Privacy Act, TEX. HEALTH & SAFETY CODE § 181.004(a), (b) (West 2022).

HIPAA covered entities.[254] That said, these laws tend to exclude both education records and student treatment records from protection.[255]For example, the Texas Medical Records Privacy Act (TMRPA) applies to any "health care facility," "clinic," "health care provider," or "person who maintains an Internet site" as well as any person who "comes into possession of protected health information" or "obtains or stores protected health information,"[256] even if that facility, clinic, provider, or person is not a HIPAA covered entity.[257] This definition would appear, at first glance, to include university-owned student health centers. However, the TMRPA specifically excludes both education records and student treatment records from protection.[258]

4. State Data Security Laws

More than two-thirds of states have modest data security laws that require the secure disposal (or destruction) of paper and/or electronic documents that contain personal identifying information, including health information.[259] As an illustration, Montana's data security law provides that a business shall take all reasonable steps "to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer necessary to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable."[260]

However, most state data security laws have limited application.[261] Some of these laws do not apply to the state or its instrumentalities, which means that

---

254 *See, e.g., id.* (stating that HIPAA covered entities shall comply with the HIPAA Privacy Rule but that non-HIPAA covered entities shall comply with the Texas Medical Records Privacy Act).

255 *See, e.g., id.*

256 *Id.* § 181.001(b)(2)(A)–(C).

257 *See id.*

258 *Id.* § 181.058(1)–(2).

259 *See, e.g.*, KY. REV. STAT. ANN. § 365.725 (West 2006) ("When a business disposes of, other than by storage, any customer's records that are not required to be retained, the business shall take reasonable steps to destroy, or arrange for the destruction of, that portion of the records containing personally identifiable information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means."). *See generally* Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 95 NOTRE DAME L. REV. 155, 198–200 (2019) (reporting the author's findings regarding the number of states that have data security laws).

260 MONT. CODE ANN. § 30-14-1703.

261 *See infra* text accompanying notes 262–66266 (explaining why state data security laws have limited application).

state universities and their student health centers would not be regulated.[262] Some of these laws do not apply to HIPAA covered entities,[263] which means that most student health centers (regardless of whether they are public or private) would not be regulated.[264] Finally, some of these laws provide that if an entity is regulated by a federal data security regulation and the entity maintains procedures for disposing of personal identifying information pursuant to that federal regulation,[265] then the entity is considered to be in compliance with the state data security law.[266] Because most student health centers are regulated by the HIPAA Security Rule (even if that Rule does not protect student treatment records),[267] most student health centers will be deemed to be in compliance with the relevant state's data security law, even if the health center is not actually in compliance with such law.

5. State Breach Notification Laws

All fifty states have breach notification laws that require certain persons and entities to notify certain individuals whose data, including health data, was the subject of a security breach, depending on the circumstances of the breach.[268] These state breach notification laws are very similar in purpose and effect to those set forth in the HIPAA Breach Notification Rule.[269] That is, they are designed to alert both the individual who is the subject of the data as well as an appropriate governmental agency of a data breach, thus enabling the individual to take self-protection measures while also providing at least one government agency the opportunity to respond and/or monitor compliance.[270]

---

[262] *See, e.g.*, CONN. GEN. STAT. ANN. § 42-471(f) (West 2017) (exempting the state and its instrumentalities from regulation); DEL. CODE ANN. tit. 6, § 5004C(4) (West 2015) (also exempting the state and its instrumentalities).

[263] *See, e.g.*, 6 DEL. CODE ANN. tit. 6, § 5004C(2) (exempting HIPAA-covered health care providers from regulation) (West 2015); HAW. REV. STAT. ANN. § 487R-2(e)(2) (also exempting the state and its instrumentalities); 9 VT. STAT. ANN. § 2445(d)(2) (same).

[264] *See supra* notes 97–102 (explaining why most student health centers are HIPAA covered health care providers).

[265] *See* 45 C.F.R. § 164.310(d)(2)(i)–(ii) (HIPAA Security Rule provisions regulating the secure disposal and destruction of ePHI).

[266] *See, e.g.*, COLO. REV. STAT. ANN. § 6-1-713(3) (West 2018).

[267] *See supra* notes 97–101 (explaining why most student health centers are HIPAA covered health care providers).

[268] *See* Tovino, *Going Rogue*, *supra* note 259, at 192–98 (finding, after a comprehensive survey, that all states have breach notification laws that require certain persons and entities to notify state residents, consumers, and other individuals whose health data was the subject of a security breach).

[269] *See supra* Part I.A.3 (summarizing the HIPAA Breach Notification Rule).

[270] *See, e.g.*, ALA. CODE §§ 8-38-5, 8-38-6 (2022).

The catch is that most state breach notification laws have limited application.[271] For example, the Alabama Data Breach Notification Act applies to any individual or institution that falls within the Act's definition of a "covered entity," defined as a "person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information."[272] At first glance, most universities' student health centers would appear to fall in this definition. After all, all state universities are government entities,[273] most private universities are non-profit organizations,[274] and the remaining private universities are for-profit corporations,[275] all of which are included within the Alabama Act's definition of "covered entity." The catch is that most state breach notification laws exempt from regulation any entity that is subject to a federal breach notification law.[276] For example, the Alabama law exempts "[a]n entity subject to or regulated by federal . . . regulations . . . on data breach notification established or enforced by the federal government" so long as the entity maintains compliance with the federal regulations.[277] Because most student health centers take insurance and bill insurance electronically, most student health centers must comply with the HIPAA Breach Notification Rule (a federal regulation).[278] Recall, however, that the HIPAA Breach Notification Rule does not apply to breaches involving student treatment records because student treatment records do not fall within the definition of uPHI.[279] The result is that a student health center will be in compliance with the HIPAA Breach Notification Rule and the state breach notification law if the center notifies

---

[271] *See id*. § 8-38-2(2).

[272] *See id*.

[273] *See id*. § 8-38-2(4) (defining government entity to include the state or any instrumentality of the state).

[274] *See, e.g.*, *Brown University of Providence, 501c3 Nonprofit Organization Information*, TAXEXEMPTWORLD, https://www.taxexemptworld.com/organization.asp?tn=45979 (last visited Feb. 5, 2023) (stating that Brown University is a nonprofit organization); *Nonprofit Organizations*, CAREER COMPASS, https://careercompass.princeton.edu/career-fields/nonprofit (last visited Feb. 5, 2023) (stating that Princeton University is a nonprofit organization); *Financial Administration, Office of the Controller*, HARV.UNIV., https://oc.finance.harvard.edu/faq/faq/tax (last visited Feb. 5, 2023) ("President and Fellows of Harvard College is exempt from federal income tax as an educational institution under Section 501(c)(3) of the Internal Revenue Code of 1986, as amended.").

[275] *See* Anne Dennon, *What Is a For-Profit College*, BEST COLLEGES (Aug. 27, 2020), https://www.bestcolleges.com/blog/what-is-a-for-profit-college/ (listing illustrative for-profit universities).

[276] *See supra* Part I.A.3 (summarizing the HIPAA Breach Notification Rule).

[277] *See* ALA. CODE § 8-38-11 (2022).

[278] *See supra* text accompanying notes 98–102 (explaining why most student health centers are HIPAA covered health care providers).

[279] *See supra* text accompanying notes 171–76.

faculty and staff of breaches of their uPHI even if the center does not notify postsecondary students of breaches of their uPHI.

6. New State Consumer Data Protection Laws

As of this writing, five states (California, Colorado, Connecticut, Utah, and Virginia) have enacted new consumer data protection laws that apply to some businesses that collect, use, disclose, and/or sell personal data, including health data.[280] These new laws give data subjects comprehensive privacy rights relating to their personal information.[281] Illustrative rights include the right to know what personal information is being collected, the right to know what personal information is sold and to whom, the right to opt out of the sale or sharing of personal information, the right to limit the use and disclosure of sensitive personal information (including health information), the right to delete personal information, the right to correct inaccurate personal information, and the right not to be retaliated against for opting out of the sale of information or the exercise of rights.[282] In addition to these privacy-related rights, these new consumer data protection laws also contain security requirements that are similar to the HIPAA Security Rule; that is, they require data controllers and processors to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.[283] Lastly, these new data protection laws internally reference state breach notification requirements that are similar to the HIPAA Breach Notification Rule.[284] In summary, these new consumer data protection laws—if applicable—would meaningfully aid in protecting the privacy and security of postsecondary students' treatment records.[285]

---

[280] *See* California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–.135 (202); Colorado Privacy Act, S.B. 21-190, 73d Leg. Reg. Sess. (2021) (codified at COLO. REV. STAT. §§ 6-1-1301 – 1313 (2023)); Connecticut Data Privacy Act, S.B. 6, Pub. Act No. 22-15 (July 1, 2023); Utah Consumer Privacy Act, S.B. 227, 2022 Gen. Sess. (2022) (codified at UTAH CODE ANN. §§ 13-61-101–404 (2023)); Virginia Consumer Data Protection Act, S.B.1392 (2021) (codified at VA. CODE ANN. §§ 59.1-571–.581).

[281] *See, e.g.*, California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–.135 (2022) (codifying a number of privacy-related rights).

[282] *See, e.g.*, *id*.

[283] *See, e.g.*, Utah Consumer Privacy Act, S.B. 227, 2022 Gen. Sess. (2022) (codified at UTAH CODE ANN.§ 13-61-302(2) (2023)); Virginia Consumer Data Protection Act, S.B.1392 (2021) (codified at VA. CODE ANN. § 59.1-574(A)(3)).

[284] Virginia Consumer Data Protection Act, S.B.1392 (2021) (codified at VA. CODE ANN. § 59.1-575(A)(2)) (requiring data processors to assist data controllers with complying with Virginia breach notification requirements).

[285] *See, e.g.*, *supra* text accompanying notes 282–84.

That said, all five consumer data protection laws require businesses to meet significant financial or data sale thresholds to be regulated.[286] For example, the California Consumer Privacy Act of 2018, the latest revisions to which went into effect January 1, 2023, only applies to businesses that have annual gross revenues in excess of twenty-five million dollars; or that annually buy, receive, sell, or share the personal information of 100,000 or more consumers; or that derive fifty percent or more of their annual revenues from selling consumers' personal information.[287] It is unlikely that most university-operated student health centers in California meet these thresholds.

Similarly, the Colorado Privacy Act (CPA), effective July 1, 2023, regulates certain data controllers (including certain health data controllers) that conduct business in Colorado or that produce or deliver commercial products or services that are intentionally targeted to residents of Colorado.[288] The CPA regulations only apply, however, if the controller processes the personal data of 100,000 consumers or more during a calendar year or derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.[289] It is unlikely that most student health centers in Colorado meet these thresholds.

Along the same lines, the Connecticut Data Privacy Act (CDPA), effective July 1, 2023, also regulates certain businesses and persons that produce products or services that are targeted to residents of Connecticut.[290] However, the CDPA regulations only apply if, during the preceding calendar year, the business or person "controlled or processed the personal data of not less than one hundred thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction" or "controlled or processed the personal data of not less than twenty-five thousand consumers and derived more than twenty-five per cent of their gross revenue from the sale of personal data."[291] It is unlikely that most student health centers in Connecticut meet these thresholds. Utah and Virginia, the fourth and fifth states that have new consumer

---

[286] *See infra* text accompanying notes 287–92 (describing the classes of businesses that are regulated by each consumer data privacy law).

[287] California Consumer Privacy Act, CAL. CIV. CODE § 1798.140 (2022).

[288] Colorado Privacy Act, S.B. 21-190, 73d Leg. Reg. Sess. (2021) (codified at COLO. REV. STAT. § 6-1-1304(1) (2023)).

[289] *Id.*

[290] Connecticut Data Privacy Act, S.B. 6, Pub. Act No. 22-15, § 2 (2023).

[291] *Id.*

data protection laws, have similar financial and data thresholds that university-owned student health centers in those states may not meet.[292]

Even if a student health center manages to meet one of these thresholds, however, all five consumer data protection laws expressly exclude institutions of higher education and/or HIPAA covered entities from regulation.[293] A university clearly meets the definition of an institution of higher education[294] and most student health centers take health insurance and bill insurance electronically, making them HIPAA covered entities as well.[295] Moreover, four of the five new laws expressly exclude information governed by FERPA, including education records and/or student treatment records, from protection.[296]

---

[292] The Utah Consumer Privacy Act, effective December 31, 2023, applies to any controller or processor who conducts business in Utah or produces a product or service that is targeted to Utah resident consumers but only if the controller or processor has: (1) annual revenue of $25,000,000 or more and either (2a) controls or processes personal data of 100,000 or more consumers or (2b) derives over fifty percent of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers. Utah Consumer Privacy Act, S.B. 227, 2022 Gen. Sess. (2022) (codified at Utah Code Ann. § 13-61-102 (2023)). The Virginia Consumer Data Protection Act, effective January 1, 2023, regulates certain businesses that conduct business in Virginia or that produce products or services that are targeted to residents of Virginia but only if, during a calendar year, the business controls or processes the personal data (including health data) of: (1) at least 100,000 consumers or (ii) at least 25,000 consumers and derives over fifty percent of gross revenue from the sale of personal data. Virginia Consumer Data Protection Act, S.B.1392 (2021) (codified at Va. Code Ann. § 59.1-572(A)).

[293] California Consumer Privacy Act, Cal. Civ. Code § 1798.145(c)(1)(B) (2022) ("This title shall not apply to any of the following: . . . a covered entity governed by the privacy, security, and breach notification rules issued by [HHS under HIPAA]"); Colorado Privacy Act, S.B. 21-190, 73d Leg. Reg. Sess. (2021) (codified at Colo. Rev. Stat. § 6-1-1304(2)(h)(I), (o) (2023)) ("This Part 13 does not apply to . . . information maintained . . . by a covered entity . . . [or] data maintained by a state institution of higher education . . . ."); Connecticut Data Privacy Act, S.B. 6, Pub. Act No. 22-15, § 3(a) (2023) ("The provisions of sections 1 to 11, inclusive, of this act do not apply to any: . . . institution of higher education . . . [or] covered entity."); Utah Consumer Privacy Act, S.B. 227, 2022 Gen. Sess. (2022) (codified at Utah Code Ann § 13-61-102(2)(c), (e) (2023)) ("This chapter does not apply to . . . an institution of higher education [or] a covered entity."); Virginia Consumer Data Protection Act, S.B.1392 (2021) (codified at Va. Code Ann. § 59.1-572(B)(iii), (v)) ("This chapter shall not apply to any . . . covered entity . . . or . . . institution of higher education.").

[294] *See, e.g.*, Connecticut Data Privacy Act, S.B. 6, Pub. Act No. 22-15, § 1(16) (2023) (defining institution of higher education as "any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees").

[295] *See supra* text accompanying notes 86–102 (explaining that most student health centers are HIPAA covered entities).

[296] *See* Colorado Privacy Act, S.B. 21-190, 73d Leg. Reg. Sess. (2021) (codified at Colo. Rev. Stat. § 6-1-1304(2)(j)(V) (2023)) ("This Part 13 does not apply to . . . personal data . . . regulated by [FERPA] . . . ."); Connecticut Data Privacy Act, S.B. 6, Pub. Act No. 22-15, § 3(b)(13) (2023) ("The following information and data is exempt from the provisions of sections 1 to 11, inclusive, of this act . . . personal data regulated by the Family Educational Rights and Privacy Act . . . ."); Utah Consumer Privacy Act, S.B. 227, 2022 Gen. Sess. (2022) (codified at Utah Code Ann. § 13-61-102(2)(m) (2023) ("This chapter does not apply to . . . personal data regulated by the federal Family Education Rights and Privacy Act . . . ."); Virginia Consumer Data Protection

As a result of these express exclusions, new consumer data protection laws do not protect student treatment records.

7. State Law Summary

In summary, state facility licensing laws, state medical record privacy laws, state data security laws, state breach notification laws, and new state consumer data protection laws are potential sources of privacy, security, and breach notification protections for the treatment records of postsecondary students. That said, most of these laws are expressly inapplicable to university-owned student health centers and/or to student treatment records in the possession of such centers. Although antiquated privacy provisions set forth in state professional practice acts do apply, these state professional practice acts: (1) do not carefully or heavily regulate the use and disclosure of student treatment records; (2) do not provide students with comprehensive rights relating to their health information, including the right to receive a notice of privacy practices, the right to request additional privacy protections, the right to correct inaccurate medical record entries, the right to receive an accounting of disclosures, the right to be notified of privacy and security breaches, or the right to mitigation of harmful effects associated with such breaches; (3) do not require the implementation of administrative, physical, or technical safeguards designed to ensure the confidentiality, integrity, and availability of ePHI; and (4) are not aggressively enforced (or enforceable) through stringent civil and criminal penalties, qui tam provisions, or private rights of action.[297] The result is minimal privacy, security, and breach notification protections for the treatment records of postsecondary students under state law.

When promulgating the HIPAA Rules in the early 2000s, HHS recognized that state privacy law was a "patchwork" that was "incomplete and, at times, inconsistent."[298] HHS also recognized that state privacy law "fail[ed] to provide a consistent or comprehensive legal foundation of health information privacy. For example, there is considerable variation among the states in the type of information protected and the scope of the protections provided."[299] Although five states have attempted to respond to this criticism by enacting stringent new

Act, S.B.1392 (2021) (codified at Va. Code Ann. § 59.1-572(C)(12)) ("The following information and data is exempt from this chapter . . . personal data regulated by [FERPA].").

[297] *See infra* Part I.C.1 (discussing the substantive limitations of state professional practice acts).

[298] *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82466 (Dec. 28, 2000).

[299] *Id.*

consumer data protection laws in the past five years, not one of these new laws provides any privacy, security, or breach notification protections for postsecondary students' treatment records.[300] The question now becomes whether student health centers make undergraduate, graduate, and professional students aware that their student treatment records lack federal privacy, security, and breach notification protections and/or suffer from weak state law protections.

II. STUDENT-PATIENT PRIVACY IN PRACTICE

Student health centers inform postsecondary students of privacy, security, and breach notification protections through a variety of means, including through specific statements made in notices of privacy practices (NOPPs), through general statements made on health center or other university web pages, and through cursory language set forth in emails, flyers, posters, brochures, and other materials (collectively health center communications). A review of illustrative health center communications reveals that postsecondary students are being provided with confusing information (at best) and misleading or incorrect information (at worst) regarding the privacy, security, and breach notification protections available for their student treatment records.

As background, the HIPAA Privacy Rule gives individuals the right to receive adequate "notice" of the uses and disclosures of their PHI that may be made by their covered entities as well as their legal rights and their covered entities' legal duties under the HIPAA Privacy Rule.[301] This "notice"—called the notice of privacy practices (NOPP)—must be written by the covered entity in plain language and must contain a number of required statements, including: (1) a sufficiently detailed description of each purpose for which the covered entity is permitted or required to use or disclose PHI without the individual's authorization; (2) a description of the types of uses and disclosures that require the patient's prior written authorization; (3) a statement that the individual has the right to request additional privacy protections; (4) a statement that the individual has the right to inspect and receive a copy of their PHI; (5) a statement that the individual has the right to amend incorrect PHI; (6) a statement that the individual has the right to receive an accounting of the covered entity's disclosures of their PHI; (7) a statement that the covered entity is required by

[300] *See supra* Part I.C.6 (examining the application of new consumer data protection laws to student treatment records).

[301] 45 C.F.R. § 164.520(a)(1) (2013).

law to maintain the privacy of the individual's PHI; and (8) a statement that individuals may complain to the covered entity and/or the Secretary of HHS if they believe their privacy rights have been violated.[302] In addition, a covered student health center must do all of the following with its NOPP: (1) have a paper copy of the NOPP available at the student health center for individuals to request to take with them; (2) post a paper copy of the NOPP in a clear and prominent location where it is reasonable to assume the NOPP will be seen by individuals who seek in-person care at the student health care; (3) post an electronic copy of the NOPP on the health center website if the health center has a website; and (4) affirmatively distribute the notice to individuals who receive care from the health center no later than each individual's date of first health care service delivery.[303]

Importantly, the NOPP tells individuals how their PHI will be used and disclosed and the rights that individuals have, but only with respect to their PHI.[304] Recall, however, that student treatment records and education records are excepted from the definition of PHI.[305] The result is that any statements made in the NOPP about privacy, security, and breach notification protections for PHI and about legal rights that individuals have with respect to their PHI are inapplicable to student treatment records.[306] The only beneficiaries of these protections and rights are non-students, such as current faculty and staff, faculty and staff retirees, dependents of faculty and staff, and dependents of students.[307] One would think that student health centers would inform students that they do not benefit from the protections and rights described in the NOPPs they create, post, and distribute. As discussed in more detail below, this is not always the case.

A. NOPPs that Fail to Distinguish Between Protections Applicable to Non-Students and Students

With respect to student health centers that provide health care to both students and non-students,[308] some NOPPs do not clarify that the protections and

---

[302] *Id.* § 164.520(b)(1)(ii)(B), (D), (E); *id.* § 164.520(b)(1)(iv)(A)–(E); *id.* § 164.520(b)(1)(v), (vi).

[303] *Id.* §§ 164.520(c)(2)(i), (iii); *id* § 164.520(c)(3)(i).

[304] *See supra* text accompanying note 302.

[305] *See supra* text accompanying notes 175–76', 194.

[306] *Id.*

[307] *See supra* text accompanying note 96 (providing examples of university-owned student health centers that provide health care to current faculty and staff, faculty and staff retirees, dependents of faculty and staff, and/or dependents of students, in addition to just students).

[308] *See id.*

rights described therein do not apply to students.[309] For example, the University of California (UC) Berkeley's student health and counseling centers provide services not only to students but also to faculty and staff employed by UC Berkeley.[310] The legal result is that the medical records of the faculty and staff are PHI protected by HIPAA while the medical records of the students are student treatment records protected neither by HIPAA nor by FERPA and only by state law.[311] UC Berkeley's NOPP, which by its own terms expressly applies to the student health and counseling centers, does not explain that students do not benefit from the privacy protections and legal rights described therein.[312] Instead, UC Berkeley follows the direction of the HIPAA Privacy Rule and uses the generic words "you" and "your" throughout its NOPP—words students reasonably could think refer to them.[313] For example, the header at the top of the UC Berkeley NOPP states, in capitalized font: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION."[314] The NOPP, at the bottom of the first page, further states, "YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION. You have the following rights regarding the health information we maintain about you . . . ."[315] Again, UC Berkeley students who read the posted NOPP, or who find the electronic NOPP online, or who are given a copy of the NOPP at their date of first service delivery[316] could reasonably think that the protections and rights described in the NOPP, including the right to access their medical records, the right to ask for a correction of incorrect or incomplete medical records, the right to know how their medical records have been shared, the right to ask for additional privacy-related restrictions, the right to ask for preferred communications, and the right to be notified of a breach, benefit them.[317] As

---

309 *Be Well at Work: Faculty/Staff Health Programs at UC Berkeley*, UC BERKELEY UNIV. HEALTH SERVS., https://uhs.berkeley.edu/bewellatwork (last visited Feb. 5, 2023) (listing a variety of health programs available to faculty and staff through UC Berkeley's Health Service).

310 *Id.*

311 *See supra* Parts I.A–B (explaining this result).

312 UC BERKELEY HEALTH, NOTICE OF PRIVACY PRACTICES, UNIVERSITY OF CALIFORNIA BERKELEY HEALTH SYSTEM 1 [hereinafter Berkeley NOPP], https://uhs.berkeley.edu/sites/default/files/npp_with_gdpr.pdf (last visited Feb. 5, 2023) (stating, "The University of California health care components consist of . . . the UC student health and counseling centers . . . .").

313 *Id.*

314 *Id.*

315 *Id.* This capitalized language is required by the HIPAA Privacy Rule. 45 C.F.R. § 164.520(b)(1)(i).

316 *See supra* text accompanying note 303 (explaining that covered student health centers are required to post a paper copy of their NOPP at their physical service delivery site, upload an electronic copy to their website if they have a website, and give patients a copy of the NOPP at the date of each patient's first service delivery).

317 Berkeley NOPP, *supra* note 312, at 1–3 (listing all of these rights).

discussed in Part I, however, neither these rights (set forth in HIPAA) nor the more discrete rights (set forth in FERPA) apply to postsecondary student treatment records.[318] In summary, UC Berkeley's NOPP is confusing at best and misleading or incorrect at worst.

Along the same lines, the Yale Student Health Department provides services not only to Yale students but also to their spouses.[319] The legal result is that the medical records of the Yale students' spouses are PHI protected by HIPAA while the medical records of the Yale students themselves are student treatment records protected neither by HIPAA nor FERPA. Like the Berkeley NOPP, the Yale NOPP does not explain that only the students' spouses (and not the students themselves) benefit from the privacy protections and legal rights described therein. Like the Berkeley NOPP, the Yale NOPP uses the generic words "you" and "your" throughout,[320] which Yale students reasonably could think apply to them. The Yale NOPP is also confusing (at best) and misleading or inaccurate (at worst).

Additional information provided by Yale on its website is also confusing and/or misleading. For example, one Yale web page states, generically, that medical records created by Yale Health are protected by HIPAA: "At Yale Health, we work hard to ensure your privacy and maintain the confidentiality of your information and medical records. Like all accredited healthcare institutions, we follow a federal law called the Health Insurance Portability and Accountability Act (HIPAA) . . . which is designed to protect the privacy and confidentiality of patient information."[321] This Yale web page does not clarify that the treatment records of Yale students are not subject to HIPAA's protections.[322] A different Yale web page states that "[t]he Family Educational Rights and Privacy Act (FERPA), a federal law, governs how university officials may use education records, including student health records."[323] This second

---

[318] *See supra* Parts I.A–B (explaining this legal result).

[319] *Yale Health: Student Health*, YALE UNIV., https://yalehealth.yale.edu/directory/departments/student-health (last visited Feb. 5, 2023) ("The Student Health Department has a long tradition of caring for students and their spouses.").

[320] *Yale Health: Notice of Privacy Practices*, YALE UNIV. [hereinafter Yale NOPP] (emphasis added), https://yalehealth.yale.edu/notice-privacy-practices (last visited Feb. 5, 2023) ("This notice describes how medical information about *you* may be used and disclosed and how *you* can get access to this information."); 45 C.F.R. § 164.520(b)(1)(i) (requiring this language).

[321] *Yale Health: Privacy Statement*, YALE UNIV., https://yalehealth.yale.edu/privacy-statement (last visited Feb. 5, 2023).

[322] *See id.*

[323] *University Privacy Office: Privacy Statement for Student Health Records*, YALE UNIV., https://privacy.yale.edu/privacy-student-health-records (last updated April 2022).

Yale web page does not clarify, however, that FERPA-related rights also do not apply to most student treatment records.[324] Yale students who find and read the first web page could reasonably think that their treatment records are protected by HIPAA when the opposite is true. Yale students who find and read the second page might think that Yale students benefit from FERPA-related rights with respect to their treatment records when the opposite usually is true.[325] In summary, information provided by Yale online is confusing at best and misleading or incorrect at worst.

Similarly, Goddard Health Services (Goddard), the student health center of the University of Oklahoma (OU), provides health care to OU students as well as to OU faculty, staff, and dependents.[326] The Author, who is on faculty at OU College of Law, has received outstanding health care at Goddard on multiple occasions. In the hands of Goddard, the Author's medical records are PHI protected by HIPAA while the Author's law students' medical records are student treatment records protected neither by HIPAA nor by FERPA.[327] The OU NOPP, which expressly applies to Goddard as well as to OU's Student Counseling Services, uses the generic words "you" and "your" throughout, which OU students could reasonably think apply to them.[328] Although the OU NOPP does not expressly state that OU students do not benefit from the protections and rights described therein, the OU NOPP does state that "it applies to health information that is protected by [HIPAA]."[329] The catch is that most undergraduate, graduate, and professional students (other than the law students who have taken the Author's HIPAA Privacy class) would not know that their treatment records are not protected by HIPAA. For this reason, the Author believes the OU NOPP is confusing at best and misleading at worst. As with the UC Berkeley and the Yale NOPPs, the OU NOPP fails to distinguish between the privacy rights and protections available to non-students and students.

---

[324] *See id*. Only those student treatment records that are disclosed for non-treatment purposes, thus reverting to education records protected by FERPA, benefit from FERPA-related rights. Because most student treatment records are not disclosed for non-treatment purposes, most student treatment records will never benefit from FERPA-related rights. *See* text accompanying *supra* notes 205–10 (explaining this result).

[325] *See* text accompanying *supra* notes 205–10 (explaining this result).

[326] *Goddard Health Services: About Us*, HEALTH SERVS. UNIV. OF OKLA., https://www.ou.edu/healthservices/about (last visited Feb. 5, 2023) (stating that the student health center "offers the convenience of an on-campus location and the commitment of a high-quality primary care staff to students, faculty, staff and their dependents").

[327] *See supra* Parts I.A–B (explaining this result).

[328] UNIVERSITY OF OKLAHOMA, NOTICE OF PRIVACY PRACTICES 1 [hereinafter Oklahoma NOPP], https://apps.ouhsc.edu/hipaa/documents/NoticePrivacyPracticesFullPage-7.22.22_001.pdf (last visited Feb. 5, 2023).

[329] *Id.*

B. NOPPs Provided by Student Health Centers that Serve Only Students

Part II.A., immediately above, explained how student health centers that treat both non-students and students can mislead students if their NOPPs do not distinguish between the rights and protections available to non-students versus students. A separate problem, created by the HIPAA Privacy Rule, exists for covered student health centers that treat only students. The problem is that the HIPAA Privacy Rule requires *all* covered entities, without exception, to create, post, and distribute their NOPPs, even if not one of the covered entity's patients benefits from the rights and protections described in the NOPP.[330] Consider the Vanderbilt University Zerfoss Student Health Center (Zerfoss), which only provides health care to Vanderbilt University students.[331] Because Zerfoss only provides health care to postsecondary students, all of Zerfoss' medical records meet the definition of student treatment records that are excluded from protection under HIPAA. Even if Zerfoss discloses a student treatment record in a way that reverts it back into an education record,[332] the record will regain protection under FERPA but remain excluded from protection under HIPAA.[333] In summary, the treatment records created by Zerfoss will never be PHI protected by HIPAA at any point in their creation, maintenance, use, or disclosure. Yet, the HIPAA Privacy Rule requires Zerfoss to have, to post, and to distribute a HIPAA NOPP.[334] Zerfoss dutifully complies with this rule by having, posting, and distributing a HIPAA NOPP.[335] Moreover, Zerfoss includes within its NOPP generic language (including "you" and "your") that is required by the HIPAA Privacy Rule.[336] Zerfoss is essentially forced by the HIPAA

---

330 *See supra* note 302 (containing no exceptions to the many NOPP requirements for covered student health centers whose only patients are students).

331 *Student Health Center*, VANDERBILT UNIV. MED. CTR., https://www.vumc.org/student-health (last visited Feb. 5, 2023) ("The Zerfoss Student Health Center is here to serve the primary care needs of the Vanderbilt student community.").

332 *See supra* text accompanying notes 205–17 (explaining when a student treatment record will revert back into an education record and regain protection under FERPA but not HIPAA).

333 *See supra* Parts I.A–B (explaining this legal result).

334 *See supra* note 303; VANDERBILT. UNIV. MED. CTR., VANDERBILT UNIVERSITY NOTICE OF PRIVACY PRACTICES, https://www.vumc.org/information-privacy-security/sites/default/files/public_files/EDocsView.pdf (last visited Feb. 5, 2023).

335 VANDERBILT UNIV. MED. CTR., *supra* note 334; *Information Privacy and Security: Notice of Privacy Practices*, VANDERBILT UNIV. MED. CTR., https://www.vumc.org/information-privacy-security/notice-privacy-practices (last visited Feb. 5, 2023) ("The HIPAA Privacy Rule mandates that health care providers distribute a Notice of Privacy Practices to all patients.").

336 45 C.F.R. § 164.520(b)(1)(i) (2022) (requiring all NOPPs to contain the following language as a header: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY") (capitalized language in original).

Privacy Rule into misleading Vanderbilt students about the protections available for their treatment records.

The same is true for other student health centers that treat only students. The Duke University Student Health Service treats only students,[337] for example, yet it is forced by the HIPAA Privacy Rule to have, to post, and to distribute an NOPP.[338] Duke has dutifully complied with HIPAA by producing an NOPP that contains generic language that Duke students could reasonably think applies to them.[339] The Wilce Student Health Center (Wilce) at Ohio State University also treats only students.[340] Wilce has dutifully complied with the HIPAA Privacy Rule by producing an NOPP that contains generic language required by the HIPAA Privacy Rule that Ohio State students could reasonably think applies to them.[341] As with Vanderbilt, Duke and Ohio State are essentially forced by the HIPAA Privacy Rule into misleading their students about the protections available for their treatment records.

C. Student Health Centers that Try to Correct for HIPAA

Some universities appear to recognize that HIPAA requires their covered student health centers to create NOPPs but that the rights and protections described therein could confuse students into thinking that their treatment records are protected by HIPAA. These universities have attempted, in one way or another, to correct for the problems created by HIPAA. Some student health centers do this by refusing to post an NOPP altogether.[342] For example, when an Internet search for an NOPP applicable to the University of Virginia (UVA) Student Health and Wellness revealed no results, the Author contacted UVA, asking for a copy of its NOPP.[343] The Author received a response from a UVA representative stating that, "[UVA] follows privacy practices as defined by the

---

[337] *See Student Health*, DUKE STUDENT AFFS., https://students.duke.edu/wellness/studenthealth/ (last visited Feb. 5, 2023) ("We offer a wide range of healthcare services for all Duke students . . . .").

[338] *See supra* text accompanying note 303.

[339] *Notice of Privacy Practices*, DUKE HEALTH, https://www.dukehealth.org/privacy (last visited Feb. 5, 2023) (stating that the Duke NOPP applies to "Duke University Student Health").

[340] *See Student Health Services*, OHIO STATE UNIV., https://shs.osu.edu/ (last visited Feb. 5, 2023) ("The Wilce Student Health Center . . . provid[es] a variety of health care services to the student population.").

[341] OHIO STATE UNIV., OFF, STUDENT LIFE, NOTICE OF PRIVACY PRACTICES, https://shs.osu.edu/documents/notice-of-privacy-practices.pdf (last visited Feb. 5, 2023).

[342] *See, e.g.*, *infra* notes 343–45

[343] Email from Stacey Tovino, Univ. of Okla., to Joyce A. Moton, Dept. of Student Health and Wellness, Univ. of Va. (Oct. 25, 2022, 10:40 AM CDT) (on file with author).

Family Educational Rights and Privacy Act (FERPA) and State Law."[344] UVA thus decided to buck HIPAA and not create or post an NOPP applicable to its student health center so as not to mislead students into thinking their records are protected by HIPAA. The catch is that FERPA's "privacy practices," cited by UVA in its email, are unfavorable to students. In particular, FERPA does not give students the right to access or correct their treatment records, and FERPA allows student treatment records to be disclosed in a dozen-plus situations (including to the student's parents if the student is a dependent under federal tax law) without the student's prior written consent.[345] More generally, student treatment records only benefit from FERPA's protections when they are disclosed for non-treatment purposes (thus reverting back into education records),[346] which rarely happens.

Other universities try to correct for HIPAA by modifying language in their NOPPs.[347] For example, Stanford University's Vaden Health Center includes the following language on the first page of its NOPP:

> If you are a student, treatment of your health information is governed by the Family Educational Rights and Privacy Act ("FERPA") and requirements of applicable California State law. The health information of all others is governed by regulations under the Health Insurance Portability and Accountability Act ("HIPAA"), as amended, and the requirements of applicable California State law. For health information covered by HIPAA, Vaden is required to provide you with this Notice and abide by this Notice with respect to health information covered by HIPAA."[348]

Similarly, New York University's (NYU's) Student Health Center includes the following language at the top of the first page of its NOPP:

> NYU Student Health Center ("SHC") is required by federal and state law to maintain the privacy of your health information. If you are a student, treatment of your health information is governed by the Family Educational Rights and Privacy Act ("FERPA") and requirements of applicable New York State law. The health information of all others is governed by regulations under the Health

---

344 Email from Leann Burns, Sr. Compliance Manager, Dept. of Student Health and Wellness, Univ. of Va., to Stacey Tovino, Univ. of Okla. (Oct. 25, 2022, 01:57 PM CDT) (on file with author).

345 *See supra* text accompanying notes 193, 206.

346 *See* text accompanying notes 205–10 (explaining this result).

347 *See infra* notes 348–51351.

348 STAN. UNIV.: STAN. VADEN HEALTH SERVS., NOTICE OF PRIVACY PRACTICES (Sept. 23, 2013), https://vadend9.sites.stanford.edu/sites/g/files/sbiybj20746/files/media/file/vaden_notice_of_privacy_practices_0.pdf.

> Insurance Portability and Accountability Act ("HIPAA"), as amended, and the requirements of applicable New York State law. For health information covered by HIPAA, SHC is required to provide you with this Notice and abide by this Notice with respect to health information covered by HIPAA.[349]

Likewise, Harvard University Health Services includes the following language on the first page of its NOPP:

> To Students: Although the Health Insurance Portability and Accountability Act privacy regulations do not apply to your medical records, those records are protected under state privacy laws, other federal laws, and in most instances will be treated in the same manner described in the HUHS Notice of Privacy Practices. In particular, Harvard College and Harvard Summer School students should note that there are special student privacy rights that apply to them that are described in their schools' student handbooks. To the extent that any conflict exists between the privacy rights contained in this notice and the privacy rights contained in those handbooks with respect to Harvard College and Harvard Summer School students, the privacy rights contained in the handbooks will control.[350]

Boston University (BU) provides similar information on its website: "STUDENTS: Please contact the BU Student Health Center with any questions about the privacy of your medical records. Student Health records are subject to FERPA. They are not subject to HIPAA's Privacy and Security rules or to the policies found on this website."[351]

Harvard is correct that HIPAA does not apply to student treatment records. Stanford and NYU are correct that FERPA "governs" student treatment records. In addition, BU is correct that student treatment records are "subject" to FERPA. The catch, again, is that FERPA's "governance" of student treatment records (or the way in which student treatment records are "subject" to FERPA) is unfavorable to students. Again, FERPA does not give postsecondary students the right to access or correct their treatment records at all[352] and FERPA allows student treatment records to be disclosed in a dozen-plus situations (including to

---

[349] N.Y.U.: NYUSTUDENTHEALTHCENTER, NOTICE OF PRIVACY PRACTICES (Apr. 13, 2013), https://www.nyu.edu/content/dam/nyu/studentHealthServices/documents/records-forms-policies/notice-of-privacy-practices.pdf.

[350] HARV. UNIV. HEALTH SERVS., NOTICE OF PRIVACY PRACTICES (June 1, 2019), https://huhs.harvard.edu/files/huhs/files/huhs_notice_of_privacy_practices.pdf.

[351] *Welcome to BU's HIPAA and Health Information Privacy Resources Site*, B.U. HEALTH INFO. PRIV. RES., https://www.bu.edu/hipaa/ (last visited Feb. 5, 2023).

[352] *See supra* text accompanying note 193.

the student's parents if the student is a dependent under federal tax law) without the student's prior written consent.[353] More generally, student treatment records only benefit from FERPA's protections when they are disclosed for non-treatment purposes (and thus revert back into education records, which rarely happens).[354] Thus, Stanford, NYU, and BU have accurately referenced a governing law, but the governing law provides no substantive protections in most cases and few protections in other cases.

In summary, this Part has explored whether postsecondary institutions make their students aware that their treatment records lack strong federal protections and/or suffer from weak state protection. This Part finds that student health centers inform postsecondary students of privacy, security, and breach notification protections through a variety of means, including through specific statements made in notices of privacy practices, general statements made on health center and other university web pages, and cursory language in emails, flyers, brochures, posters, and other materials (collectively health center communications). This Part has shown that many health center communications: (1) fail to adequately distinguish between the significant protections available for the medical records of non-students and the limited protections available for student treatment records; or (2) incorrectly state or suggest that all student health center patients have stringent protections. The following Part corrects the lack of protection for student treatment records and provides justification for these corrections.

III. REFORM JUSTIFICATION

In the preamble to the final HIPAA Privacy Rule published in December 2000, HHS recognized that its decision not to protect student treatment records under HIPAA was unfair to students because they would not have the same privacy rights and protections as other patients.[355] HHS also admitted that it considered protecting student treatment records under HIPAA until the time such records reverted back to education records protected by FERPA.[356] HHS

---

353 *See supra* text accompanying note 205.

354 *See supra* text accompanying notes 205–10 (explaining this result).

355 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82483 (Dec. 28, 2000) ("[W]e strongly believe every individual should have the same level of privacy protection for his/her individually identifiable health information . . . .").

356 *Id.* ("[W]e considered requiring health care providers engaged in HIPAA transactions to comply with the privacy regulation up to the point these records were used or disclosed for purposes other than treatment. At that point, the records would be converted from protected health information into education records. This conversion would occur any time a student sought to exercise his/her access rights. The provider, then, would

ultimately decided not to protect student treatment records under HIPAA at any point for two reasons. First, HHS thought that it would be "unduly burdensome to require providers to comply with two different, yet similar, sets of regulations;" that is, HIPAA and FERPA.[357] Second, HHS thought that, because FERPA excluded student treatment records from federal protection (leaving them only to state law), HIPAA should too.[358] Neither of these justifications can stand.

A. HHS Underestimated the Number of Laws with Which Student Health Centers Must Comply

With respect to the rationale that requiring student health centers to comply with *two* different sets of regulations would be unduly burdensome, HHS completely failed to recognize that most student health centers would have to comply with *three* different sets of regulations because they treat non-students.[359] That is, most student health centers have to comply with HIPAA with respect to their non-student patients, state law with respect to their student patients whose records are used or disclosed only for treatment purposes, and FERPA with respect to their student patients whose records are disclosed for non-treatment purposes.[360] HHS also failed to realize how difficult it would be for most student health centers to understand this extraordinarily confusing patchwork of federal and state privacy law and to accurately convey this law to patients through notices of privacy practices and other print and electronic communications. The result is that many student health centers confuse their student patients into thinking that their treatment records are protected by HIPAA and/or FERPA when their records may be protected only by state law.[361]

---

need to treat the record in accordance with FERPA's requirements and be relieved from its obligations under the privacy regulation."); *see supra* text accompanying notes 205–10 (explaining when student treatment records revert back to education records and become protected by FERPA).

357 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82483.

358 *See id*. ("Congress did not specifically provide [HHS] with authority to disturb the scheme it had devised for records maintained by educational institutions and agencies under FERPA. We do not believe Congress intended to amend or preempt FERPA when it enacted HIPAA.").

359 *Id.*

360 *See supra* Part I.A (explaining that HIPAA applies to covered student health centers that create and maintain non-student medical records); *supra* text accompanying note 16 (explaining that state law applies to student treatment records that are not disclosed for a reason other than treatment purposes); *supra* text accompanying notes 205–10 (explaining that FERPA applies to student treatment records disclosed for non-treatment purposes).

361 *See supra* Parts II.A–B (reporting that some student health center NOPPs fail to distinguish between the protections and rights that apply to non-students and students; reporting that other student health centers create, post, and distribute NOPPs when none of their patients benefit from any of the protections or rights described in the NOPPs).

If federal law were amended such that HIPAA applied to student treatment records, regardless of how they were subsequently used or disclosed, that would reduce the number of laws with which student health centers have to comply from three to one; that is, just HIPAA. In addition, the NOPPs of student health centers that do not differentiate between the protections available to student and non-student patients would now be accurate.

B. Post-FERPA Technological Advances Demand Greater Data Privacy, Security, and Breach Notification Protections

Also flawed is HHS's reasoning that because FERPA excluded student treatment records from federal protection in 1974, leaving them only to state law, HIPAA should too. This reasoning is unsound because post-1974 technological advances demand significantly stronger privacy, security, and breach notification protections.[362] In 1974, the year Congress enacted FERPA, paper medical records were the norm.[363] Although it is not impossible to breach the privacy and security of paper records, electronically maintained information is particularly vulnerable to large-scale breaches followed by widespread (and unauthorized) uses, disclosures, and/or sales.[364] Smart phones, also not available in 1974, have increased the ease with which a student's health information can be quickly photographed, screenshotted, emailed, texted, voiced, or videoed by a worker (including a student worker) at a student health center and disclosed to an unauthorized third party (including other students) or spread via social media.[365] Indeed, in its recently released 2023 cybersecurity adversary report, SOPHOS reported that ninety-four percent of organizations experienced a cybersecurity attack of some form in 2022.[366] Today's new digital landscape begs for greater privacy, security, and breach notification protections for student treatment records.[367]

---

[362] *See infra* text accompanying notes 363–67.

[363] *See* Family Educational Rights and Privacy Act, Pub. L. No. 93-380, § 513, 88 Stat. 571–74 (1974) (codified at 20 U.S.C. § 1232g); Evans, *supra* note 36.

[364] *See, e.g.*, Liu, *supra* note 37; *see supra* text accompanying notes 48–56.

[365] *See* Ng, *supra* note 38.

[366] THE STATE OF CYBERSECURITY 2023, THE BUSINESS IMPACT OF ADVERSARIES 1 (2023), https://www.sophos.com/en-us/whitepaper/state-of-cybersecurity.

[367] *See* Grande, *supra* note 39.

C. Privacy, Security, and Breach Notification Protections Are Needed to Combat the Stigma Associated with the Services for which Postsecondary Students Seek Treatment

The fact that HIPAA does not protect the privacy and security of student treatment records is also concerning given the stigma, shame, and prejudice associated with many physical and mental health conditions for which postsecondary students seek treatment.[368] STIs remain heavily stigmatized, even in an era of sex positivity,[369] and STI-related stigma and shame have been found to undermine STI testing, treatment, and partner notification.[370] Mental health conditions and substance use disorders also are associated with significant shame, stigma, and prejudice that can interfere with diagnosis, treatment, and recovery.[371] In both contexts, public health experts recommend strengthening privacy and security protections as a means of combating screening and treatment hesitancy.[372]

D. Strengthened HIPAA Privacy Protections for Reproductive Health Information Must Benefit Students Too

Current political realities relating to reproductive health care also weigh in favor of strong privacy, security, and breach notification protections for students' reproductive health records.[373] Since the Supreme Court's June 2022 decision in *Dobbs v. Jackson Women's Health Care*,[374] thirteen states have criminalized most abortions and Georgia has banned abortions at approximately six weeks.[375] On April 17, 2023, HHS released a proposed rule that, if finalized, would increase the protections available under the HIPAA Privacy Rule for PHI that is reproductive in nature.[376] In particular, the proposed rule would prohibit a HIPAA covered entity from using or disclosing PHI: (1) where the use or disclosure is for a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing,

---

368 *See, e.g.*, Bickham, *supra* note 26; Barth, *supra* note 26.

369 *See, e.g.*, Gunter, *supra* note 27.

370 *See, e.g.*, Morris, *supra* note 28.

371 *See, e.g.*, Borenstein, *supra* note 29; *Reframing Shame*, *supra* note 29; Pescosolido, *supra* note 29.

372 *See, e.g.*, Leichliter, *supra* note 30; *Reducing Stigma*, *supra* note 30. *See generally* Clement, *supra* note 30.

373 *See infra* notes 374–79.

374 *See* 597 U.S. __, *5 (2022) ("The Constitution makes no reference to abortion, and no such right is implicitly protected by any constitutional provision[.]") (internal references and citations omitted).

375 *See Tracking the States Where Abortion Is Now Banned*, *supra* note 34.

376 U.S. Dep't of Health & Hum. Servs., HIPAA Privacy Rule to Support Reproductive Health Care Privacy, Notice of Proposed Rulemaking, 88 Fed. Reg. 23506 (Apr. 17, 2023) (to be codified at 45 C.F.R. pt. 160, 164).

or facilitating reproductive health care (hereinafter, reproductive investigation or proceeding); or (2) to identify any person for the purpose of any reproductive investigation or proceeding.[377] The proposed rule clarifies that seeking, obtaining, providing, or facilitating reproductive health care includes, but is not limited to, "expressing interest in, inducing, using, performing, furnishing, paying for, disseminating information about, arranging, insuring, assisting, or otherwise taking action to engage in reproductive health care; or attempting any of the same."[378] The protections of the proposed rule would apply where one or more of the following conditions exists: (1) the relevant criminal, civil, or administrative investigation or proceeding is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care outside of the state where the investigation or proceeding is authorized and where such health care is lawful in the state in which it is provided; or (2) the relevant criminal, civil, or administrative investigation or proceeding is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care that is protected, required, or authorized by Federal law, regardless of the state in which such health care is provided; or (3) the relevant criminal, civil, or administrative investigation or proceeding is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care that is provided in the state in which the investigation or proceeding is authorized and that is permitted by the law of that state.[379] If HHS finalizes this proposed rule as it is currently written, the result will be that the HIPAA Privacy Rule will provide greater privacy protections for reproductive health information compared to other information. However, postsecondary students who receive reproductive health care services at their student health centers will not benefit from these strengthened protections unless the exception for student treatment records is removed from the HIPAA Privacy Rule.

E. Geographic Diversity at Postsecondary Institutions Weighs in Favor of the Application of Strong Federal Law

The lack of federal protection for student treatment records is also troubling given the significant number of undergraduate, graduate, and professional students who cross state lines to attend out-of-state institutions, including military institutions, non-military public institutions, and private institutions. Ninety-five percent of the students who attend the U.S. Coast Guard Academy

377 *Id.* at 23552.
378 *Id.*
379 *Id.*

come from outside Connecticut, 94% of the students who attend West Point come from outside New York, and 93% of the students who attend the Naval Academy and the Air Force Academy come from outside Maryland and Colorado, respectively.[380] Yet these students' treatment records are protected only by Connecticut, New York, Maryland, or Colorado law, even though these students are not residents of those states.[381] Geographic diversity is also high at many non-military public institutions. For example, 75% of University of Vermont students come from outside Vermont, 63% of University of Alabama students come from outside Alabama, 59% of University of Rhode Island students come from outside Rhode Island, and 57% of University of Mississippi students come from outside Mississippi.[382] Yet these students' treatment records are protected only by Vermont, Alabama, Rhode Island, or Mississippi law, as the case may be.[383] Geographic diversity is high at many private universities as well.[384] Ninety-six percent of Brown University students come from outside Rhode Island, 84% of Tulane University students come from outside Louisiana, and 82% of Princeton University students come from outside New Jersey.[385] Again, the treatment records of these out-of-state students are protected only by the laws of the state in which their postsecondary institution are located, even though these students did not have the ability to vote on the legislators who introduced these laws and likely had little opportunity to influence the passage of these laws prior to their arrival on.[386] While in-state students may have some understanding of the privacy laws in their state due to news media or otherwise, out-of-state students are less likely to be aware of the substantive protections available (or not) through state law. This lack of comprehension may be reinforced or perpetuated by misleading language in student health centers' NOPPs.

---

[380] *Percentage of Out-of-State Students at Public Universities*, COLLEGEXPRESS [hereinafter College Express], https://www.collegexpress.com/lists/list/percentage-of-out-of-state-students-at-public-universities/360/ (last visited Feb. 5, 2023).

[381] *See supra* Parts I.A–B (explaining this result).

[382] *Id.*

[383] *See infra* note 385.

[384] *See supra* Parts I.A–B (explaining this result).

[385] *See, e.g.*, *Brown Demographics & Diversity Report*, COLL. FACTUAL, https://www.collegefactual.com/colleges/brown-university/student-life/diversity/ (last visited Feb. 5, 2023); *Tulane Demographics & Diversity Report*, COLL. FACTUAL, https://www.collegefactual.com/colleges/tulane-university-of-louisiana/student-life/diversity/ (last visited Feb. 5, 2023); *Princeton Demographics & Diversity Report*, COLL. FACTUAL, https://www.collegefactual.com/colleges/princeton-university/student-life/diversity/ (last visited Feb. 5, 2023).

[386] *See supra* Parts I.A–B (explaining this result).

F. Universities Heavily Encourage Postsecondary Students to Use Student Health Centers

Finally, once postsecondary students arrive on campus, they are heavily persuaded by faculty, staff, and other university representatives to seek mental health care, reproductive health care, infectious disease, and other sensitive health services on campus, at the student health center.[387] Indeed, college, graduate, and professional students are flooded with emails,[388] posters,[389] flyers,[390] brochures,[391] and other communications that identify free or discounted services[392] available at the student health center and that advertise confidential appointments[393] for such services. Many of the advertised services are especially sensitive and/or stigmatizing in nature, including mental health and substance use disorder services,[394] gynecology-oncology services,[395] pregnancy testing services,[396] HIV and sexually transmitted infection services,[397] and other infectious disease services.[398] Rarely, if ever, do these university-sponsored communications clarify the privacy, security, and breach notification costs to students of seeking care at the student health center rather

---

[387] *See infra* notes 388–98398.

[388] *See, e.g.*, Email from Katherine Qualls Fay, Okla. Univ. Health Servs., to Kale Parker, student, Okla. Univ. Coll. of Law, re: OUMM: Another chance to get a flu shot! (Jan. 24, 2023, 09:28 CST) [hereinafter OU Email] (on file with author); Email from Katherine Qualls Fay, Okla. Univ. Health Servs, to Becca Schmidt, student, Okla. Univ. Coll. of Law, re: OUMM: Free HIV Testing on Campus (Feb. 7, 2023, 11:49 CST) [hereinafter OU Email 2] (on file with author).

[389] *See, e.g.*, poster, UNIV. AT BUFFALO, GETTING HELP FOR YOUR MENTAL WELLNESS [hereinafter Buffalo Poster] (on file with author); poster, UNIV. SOUTH ALA., STUDENT HEALTH CTR. [hereinafter South Alabama Poster] (on file with author).

[390] *See, e.g.*, flyer, UNIV. WISC. MADISON, STUDENT HEALTH & WELLNESS CTR., STRESSED THIS WEEK (on file with author); flyer, CUNY, THE WELLNESS CENTER STUDENT HEALTH SERVICES [hereinafter CUNY Flyer] (on file with author).

[391] *See, e.g.*, brochure, UNIV. OF WISC. RIVER FALLS, STUDENT HEALTH SERVICES BROCHURE (May 2021) [hereinafter UW-RF Brochure] (on file with author); brochure, UNIVERSITY OF TEXAS AT AUSTIN GRADUATE STUDENT MENTAL HEALTH SERVICES BROCHURE (Fall 2020) [hereinafter UT Brochure] (on file with author).

[392] *See, e.g.*, Email from Human Resources, University of Oklahoma, to Becca Schmidt, student, Univ. Okla. Coll. of Law, re: Student Health Plan—Enroll by Feb. 1 (Jan. 25, 2023, 13:53 CST) (on file with author) (stating that University of Oklahoma (OU) students who have student health insurance can receive free office visits at Goddard Health Center, OU's on-campus student health center).

[393] *See, e.g.*, OU Email 2, *supra* note 388 (stating that the OU student health center "will provide free, rapid, and confidential HIV testing").

[394] *See, e.g.*, Buffalo Poster, *supra* note 389; UT Brochure, *supra* note 391, at 3.

[395] *See, e.g.*, CUNY Flyer, *supra* note 390.

[396] *See, e.g.*, UW-RF Brochure, *supra* note 391, at 2.

[397] *See, e.g.*, *id.*; South Alabama Poster, *supra* note 389; OU Email 2, *supra* note 388.

[398] *See, e.g.*, OU Email, *supra* note 388.

than an independent, off-campus health care facility.[399] To the contrary, and as discussed in Part II, many students are provided a HIPAA Notice of Privacy Practices at the beginning of their first student health center visit.[400] Frequently, this notice will state or suggest that student treatment records are protected by HIPAA and that students have rights enforceable by HHS in the event of a privacy or security breach when the opposite is true.[401] To prevent postsecondary students from being confused or misled going forward and to strengthen the privacy, security, and breach notification protections available to postsecondary students, HHS and Congress must amend HIPAA and FERPA, respectively.

IV. PROPOSALS

Currently, HIPAA defines PHI as individually identifiable health information; that is, information that: (1) "[i]s created or received by a health care provider, health plan, employer, or health care clearinghouse"; and (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual[,] the provision of health care to an individual[,] or the past, present, or future payment for the provision of health care to an individual"; and that either (i) "identifies the individual"; or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."[402] Currently, HIPAA excepts student treatment records from the definition of PHI.[403] The exception for student treatment records must be removed, as indicated by the following stricken (deleted) and italicized (added) language:

> Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; ~~(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv)~~; (ii~~i~~) In employment records held by a covered entity in its role as employer; and (i~~v~~*ii*) Regarding a person who has been deceased for more than 50 years.[404]

---

[399] Not one of the university-sponsored communications referenced in *supra* notes 388–91 informs students that their treatment records are not protected by HIPAA and/or that their treatment records could be protected by HIPAA if they received their care at an off-campus health care facility.

[400] *See supra* Part II (referencing a number of university NOPPs that contain these statements or suggestions); *supra* Parts I.A–B (explaining that neither HIPAA nor FERPA protects student treatment records).

[401] *See supra* Parts I.A–B.

[402] 45 C.F.R § 160.103 (defining protected health information).

[403] *Id.* (defining protected health information and excluding from that definition student treatment records).

[404] *Id.* (defining protected health information).

The result will be that all student treatment records maintained by a student health center (regardless of whether and how they are subsequently used or disclosed) will be protected by the HIPAA Privacy Rule (regardless of whether they are paper or electronic), the HIPAA Security Rule (if they are electronic) and the HIPAA Breach Notification Rule (if they are unsecured).[405]

Recall, however, that FERPA defines a student treatment record as a postsecondary student's health record that has not been disclosed for non-treatment purposes, which is extraordinarily confusing.[406] For example, if a postsecondary student voluntarily consents to the disclosure of her treatment record to a potential employer for a job-related purpose, the record loses its status as a student treatment record and reverts to an education record, protected only by the limited rights set forth in FERPA. A student's consensual disclosure of her medical record should not result in the loss of HIPAA protections. Indeed, if the Author (a non-student) consents to the disclosure of her own medical records at the student health center, they do not lose HIPAA-protected status. The same should be true of student medical records. Therefore, Congress must amend FERPA, as indicated by the following stricken (deleted) and italicized (added) language:

> The term "education records" does not include—
>
> (i) records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute;
>
> (ii) records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement;
>
> (iii) in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or
>
> (iv) records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are ~~made or~~ maintained by ~~a~~ *an educational agency or institution on behalf of an*

---

405 *See supra* text accompanying notes 144–46 (explaining the application of the HIPAA Rules).

406 *See supra* text accompanying notes 205–10 (explaining how student treatment records revert to education records protected by FERPA when they are disclosed for non-treatment purposes).

> *employed or contracted* physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in *a* ~~his~~ professional or paraprofessional capacity, or assisting in that capacity.~~, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice~~.[407]

The legal result of this amendment is that postsecondary students' treatment records will receive the stronger protections in HIPAA, not the weaker protections in FERPA, regardless of whether they are further used or disclosed for treatment or non-treatment purposes.

The statutory and regulatory amendments offered in this Part are straightforward and should be enacted by Congress and promulgated by HHS, respectively, as soon as possible. In the meantime, student health centers should amend their NOPPs and other online and print materials to clarify how student treatment records actually are protected under the law. The language used by Stanford, NYU, Harvard, and BU[408] is recommended until such time as Congress amends FERPA and HHS amends the HIPAA Rules in accordance with this Article.

CONCLUSION

This Article has carefully untangled a complex web of federal and state privacy, security, and breach notification laws potentially applicable to postsecondary student treatment records. This Article has shown that most postsecondary student treatment records are protected neither by HIPAA nor FERPA. Instead, most postsecondary student treatment records are protected by weak and uneven state laws that: (1) do not carefully or heavily regulate the use and disclosure of student treatment records; (2) do not provide students with

---

[407] 20 U.S.C. § 1232g(A)(4)(B)(iv). The regulations implementing FERPA also would need to be changed, as follows: "Education records. . . . (b) The term does not include . . . Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are~~: (i) Made or~~ *maintained by an educational agency or institution on behalf of an employed or contracted* physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in a ~~his or her~~ professional capacity or assisting in a paraprofessional capacity. ~~(ii) Made, maintained, or used only in connection with treatment of the student; and (iii) Disclosed only to individuals providing the treatment.~~ For the purpose of this definition, 'treatment' does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution[.]" 34 C.F.R. § 99.3 (2022).

[408] *See supra* Part II.C.

comprehensive rights relating to their health information, including the right to receive a notice of privacy practices, the right to request additional privacy protections, the right to correct inaccurate medical record entries, the right to receive an accounting of disclosures, the right to be notified of privacy and security breaches, or the right to mitigation of harmful effects associated with such breaches; (3) do not require the implementation of administrative, physical, or technical safeguards designed to ensure that confidentiality, integrity, and availability of student health information; and (4) are not aggressively enforced (or enforceable) through stringent civil and criminal penalties, qui tam provisions, or private rights of action.

This Article also has shown that student health centers inform postsecondary students of privacy, security, and breach notification protections through a variety of means, including through specific statements made in notices of privacy practices, general statements made on health center or other university web pages, and through cursory language set forth in emails, flyers, posters, brochures, and other materials. These materials are confusing (at best) and misleading or incorrect (at worst). To minimize student confusion and to maximize the privacy, security, and breach notification protections available for student treatment records, this Article has proposed important revisions to HIPAA's definition of protected health information and FERPA's definition of education records. These revisions should be implemented by Congress and HHS as soon as possible. In the meantime, student health centers should amend their NOPPs and other online and print materials to clarify that most student treatment records are protected only by weak state law.