Houston Journal of Health Law & Policy

HAVE YOU SEEN MY PRIVATE RIGHT OF ACTION?: CREATING A PRIVATE RIGHT OF ACTION UNDER THE HIPAA PRIVACY AND ENFORCEMENT RULES

Zachary Nye, JD, LLM

THE STATE OF MEDICAL PRIVACY BEFORE HIPAA

The family doctors of yesteryear were guardians of medical secrets who kept paper records about their patients sealed away in big file cabinets. Every patient's private health information[1] was hand-written, stored under lock and key, and rarely (if ever) left the brick and mortar confines of the physician's practice. Those days are over. Every day, our private health information is being collected, shared, analyzed, and stored with few legal safeguards.

Innovations in our healthcare delivery system mean that we have to place our trust in complex networks of insurers and a whole host of different healthcare professionals.[2] The increased use of the internet in healthcare causes our private health information to travel quickly from doctors to hospitals to insurance companies.[3] Our understanding of the human genome has taken us to a whole new world of genetic tests that have the potential to either help prevent and treat disease or reveal our most personal secrets and hidden biological traits. Our private

1 64 Fed. Reg. 59918-01 (Nov. 3, 1999) (defining private health information as "individually identifiable health information maintained or transmitted in connection with certain administrative and financial transactions").

2 U.S. DEP'T OF HEALTH & HUMAN SERVICES, *Confidentiality of Individually Identifiable Health Information* 2 (1997), https://aspe.hhs.gov/report/confidentiality-individually-identifiable-health-information.

3 *Id.*

health information is no longer protected by just locking up the office doors at night.

No federal law regulating the protection of private health information existed before 1996.[4] At that time, many other countries regulated personal privacy broadly and uniformly, while the United States' privacy regulation consisted of a series of various laws, specific to their respective industries.[5]

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Eventually, Congress decided something needed to be done to protect private health information—people's most sensitive information.[6] The individuals and entities that collect, use, and disclose health data are vast in both number and variety, so placing them all under the umbrella of one regulation was a herculean task.[7] The Common Rule,[8] passed in 1981, imposed some requirements on the use of health information in research, but federal regulations explicitly addressing the privacy of patients' health information were still absent.[9]

---

4 Daniel J. Solove, *HIPAA Turns 10: Analyzing the Past, Present and Future Impact,* JOURNAL OF AHIMA 84, no.4 (April 2013): 22-28.

5 *See generally* Daniel J. Solove & Chris J. Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357 (starting in the 1970s, Congress passed several privacy statutes that protected driver license records, school records, phone records, cable TV records, even a federal law regulating the privacy of video rental records, yet, there was not one regulation for the privacy of health records).

6 *HIPAA Turns 10*, *supra* note 4.

7 *Id.*

8 OFF. FOR HUMAN RESEARCH PROTECTIONS, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *Federal Policy for the Protection of Human Subjects ('Common Rule'),* (Mar. 18, 2016), https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html (defining "The Common Rule" as the term used by eighteen federal agencies who have adopted the same regulations governing the protection of human subjects of research. The Common Rule governs most federally funded research conducted on human beings and aims to ensure that the rights of human subjects are protected during a research project, historically focusing on protection from physical and mental harm by stressing autonomy and consent.).

9 INSTITUTE OF MEDICINE, BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH, (Sheryl J. Nass et al. eds., 2009) [hereinafter BEYOND THE HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was born of a time when the healthcare industry needed new standards regarding the management of healthcare data.[10] HIPAA included rules regarding the portability of medical information and the establishment and protection of a patient's right to medical privacy. HIPAA proposed a way to enact standards for the protection of private health information.[11] HIPAA was passed and signed into law by President Bill Clinton on August 21, 1996.[12]

HIPAA was passed with the intent of making healthcare delivery more efficient and increasing the number of Americans covered by health insurance.[13] The three main provisions of HIPAA—the portability , tax , and administrative simplification provisions—were meant to achieve these objectives.

The administrative simplification provisions of HIPAA instructed the Secretary of the U.S. Department of Health and Human Services (HHS) to issue regulations concerning electronic transmission of health information, which, due to the exponential growth of the internet's popularity, was expanding considerably in the early 1990s.[14] The primary purpose of these provisions was to standardize the use of electronic health information, but Congress also recognized that the advances in internet technology could threaten the privacy of health information.[15] Accordingly, HIPAA necessitated the creation of nationwide security standards and protections for the use of electronic healthcare information.[16] HIPAA also created the HIPAA Privacy Rule, which provides privacy standards for protected health information.[17]

PRIVACY RULE].

10 *Id.*

11 *Id.*

12 OFF. FOR CIVIL RIGHTS, US DEP'T OF HEALTH AND HUMAN SERVICES, *Summary of the HIPAA Privacy Rule* (July 26, 2013), www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

13 BEYOND THE HIPAA PRIVACY RULE, *supra* note 9.

14 *Id.*

15 *Id.*

16 *Id.*

17 Protected health information is personally identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other

Section 1172(b) of HIPAA provides that "any standard adopted under this part[18] shall be consistent with the objective of *reducing the administrative costs of providing and paying for health care*."[19] The entities subject to the rules would experience considerable up-front and enduring administrative costs for these privacy standards.[20] Though, even when considered in a vacuum, the privacy rules and standards should produce administrative and other cost savings that would exceed any amount needed to offset their costs on a national basis.[21]

The privacy and security standards authorized by HIPAA[22] were necessary due to the technological advances in information exchange facilitated by the remaining Administrative Simplification standards for the healthcare industry.[23] The same technological advances that led to enormous administrative cost savings for the industry have also made it possible to breach the security and privacy of health information on an enormous scale.[24]

By enacting the security and privacy provisions of the law, Congress recognized that adequate protection of the security and privacy of health information is an absolute necessity of the increased efficiency of information exchange brought about by the increasing prevalence of internet-connected healthcare.[25] If the privacy rules proposed were to impose net costs, they would still be "consistent with" the objective of reducing administrative costs for the health care system as a whole.[26]

---

form or medium. 20 U.S.C. 1232(g)(a)(4)(B)(iv) (excluding education records covered by the Family Educational Rights and Privacy Act, records described, and employment records held by a covered entity in its role as employer).

18 Health Insurance Portability and Accountability Act, 42 U.S.C. § 1172(b) (1996).

19 *Id.*

20 Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918-011999 (to be codified at 45 C.F.R. § 160 and § 164) [hereinafter Standards for Privacy].

21 *Id.*

22 42 U.S.C. § 1173(d) (2008).

23 U.S. DEP'T OF HEALTH AND HUMAN SERVICES, *HIPAA For Professionals*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/index.html (last visited Mar. 7, 2018).

24 Sara Heath, *Majority of 2015 Healthcare Data Breaches Due to IT Hacking*, HEALTHIT SECURITY (Feb. 9, 2016), https://healthitsecurity.com.

25 Standards for Privacy, *supra* note 20, at 12.

26 42 U.S.C. § 1173(a)(1)(B).

HIPAA'S PRIVACY RULE

Though HIPAA was passed in 1996, the actual details of the law left future specifications to Congress and the Secretary of HHS. The Privacy Rule was first proposed for public comment in 1999.[27] As of 2006, the Enforcement Rule specification was the last part of HIPAA finalized in detail.[28]

The HIPAA Privacy Rule was finally passed in 2002.[29] The volume of comments received, and the change in the leadership of the executive branch following the 2000 Presidential election, resulted in several iterations, modifications, and compromises.[30] One of the most significant demands of the Privacy Rule was that it required most healthcare providers and health plans to comply with the final version of the HIPAA Privacy Rule by April 14, 2003.[31] Smaller health plans were given until April 14, 2004, to comply.[32]

WHO IS COVERED BY THE HIPAA PRIVACY RULE?

A person or organization subject to HIPAA and its Privacy Rule is known as a "covered entity."[33] A covered entity is defined as "a health

27 BEYOND THE HIPAA PRIVACY RULE, *supra* note 9.

28 HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 32 (codified at 45 C.F.R. parts 160 and 164).

29 Solove, *supra* note 4.

30 *Id.*

31 *Id.*

32 45 C.F.R. parts 160 and 164 at 8390.

33 45 CFR § 160.103 (2016).

plan,[34] a health care clearinghouse,[35] or a healthcare provider,[36] that transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard."[37] HIPAA defines "health care" with exceptional breadth. The large category encompasses care, services, or supplies related to the health of an individual.[38] The definition includes (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, palliative care, as well as any "counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body" and (2) the "dispensing of a drug, device, equipment, or other item in accordance with a prescription."[39] To say that it is difficult to be involved in the business of healthcare and *not* be considered a "covered entity," would be an understatement.

WHAT THE HIPAA PRIVACY RULE IS LACKING

The Secretary of HHS, under Section 264 of HIPAA, provided recommendations to Congress to protect the privacy and confidentiality of personal medical records.[40] The recommendations

---

34 Section 2791(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)); 45 C.F.R. § 160.103 (2016) (defining "health plan"as an individual or group plan that provides, or pays the cost of, medical care).

35 45 CFR § 160.103 (2016) (defining "healthcare clearinghouse" as a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and value-added networks and switches, that does either of the following functions: (1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity).

36 *Id.* (defining "healthcare provider" as a provider of services, as defined in section 1861 of the Act, 42 U.S.C. 1395x(u), a provider of medical or health services, as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.).

37 45 C.F.R. § 160.103 (2016).

38 *Id.*

39 *Id.*

40 OFF. OF THE ASSISTANT SEC'Y FOR PLANNING & EVALUATION, CONFIDENTIALITY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (Oct. 5, 2016), https://aspe.hhs.gov/report/confidentiality-individually-identifiable-health-information.

ask for the enactment of federal legislation that would establish a basic national standard of protection, with clear guidance and significant incentives for the fair treatment of personal information by those in the healthcare industry, and real penalties for misuse.[41] These provisions would include: requirements that organizations entrusted with health information protect against deliberate or inadvertent misuse or disclosure; that providers give patients a clear, written explanation of how the information will be used, kept, and disclosed; that those who misuse personal health information are punished and those persons harmed have redress; and that the protection of privacy is balanced with public responsibility to support national public health priorities.[42]

Currently, under the HIPAA Privacy Rule, there is no private right of action. A patient whose private health information is misused or improperly disclosed has no means, under HIPAA, to seek recourse for that misuse or improper disclosure.[43] A patient would need to look to state law claims that are available in the patient's state or the state in which the breach occurred.[44] Possible claims include negligence claims and the violation of physician/patient confidentiality. There may also be claims for invasion of privacy (public disclosure of private facts), and invasion of privacy (intrusion into personal seclusion). However, these claims do not exist in some states.[45]

Nevertheless, most (if not all) common law claims will require a proof of damages, which may be hard or impossible to show.[46] Further, the damages alleged *must* be tied to the improper access and disclosure of the private health information.[47] To prove these damages, the injured party would need to present: paid doctors' bills; paid mental

---

41 *Id.*

42 *Id.*

43 *Id.*

44 *Id.*

45 Wendy Tannenbaum, *A Recent Decision Calls False Light Outdated*, REPORTERS' COMMITTEE FOR FREEDOM OF THE PRESS, THE NEWS MEDIA & THE LAW (Oct. 31, 2011), www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-fall-2002/recent-decision-calls-false-l.

46 George F. Indest, *Remedies for Violation of HIPAA Privacy Rights and Medical Confidentiality*, THE HEALTH LAW FIRM (2007), www.thehealthlawfirm.com/resources/health-law-articles-and-documents/Remedies-for-Violation-of-HIPAA-Privacy-Rights-and-Medical-Confidentiality.html.

47 *Id.*

health counseling fees; the purchase of credit protection insurance; the purchase of identification theft insurance; the costs incurred due to a "stolen identity"; lost compensation from time off (i.e., pay stubs, W-2 forms, 1099 forms, etc.); lost compensation from a lost job (again, with pay stubs, W-2 forms, 1099 forms, etc.); attorney's fees paid as a direct result of the breach of privacy; or other out-of-pocket expenses realized as a direct result from the breach of confidentiality or improper disclosure of private health information.[48]

FEDERAL LEGISLATION PROVIDING FOR A PRIVATE RIGHT OF ACTION UNDER HIPAA'S PRIVACY RULE IS NECESSARY

Ubi jus, ibi remedium; Latin for "*where there is a right, there's a remedy*." A right protects you only insofar as you have a remedy for its violation.[49] This is a legal principle cited and referenced in *Marbury v. Madison* and is a cornerstone upon which American jurisprudence is built.[50] Federal statutes can explicitly grant enforcement powers to private parties, but many times statutes are silent on this question. Where the statute is silent, federal courts will occasionally imply private rights of action, arguing that the structure of the statute or some other policy consideration suggests that Congress *intended* private parties to be able to sue to enforce it.[51] For example, Section10(b)(5) of the Securities Exchange Act does not expressly grant a private right of action.[52] If the Supreme Court had not implied a private right of action, then only the SEC could sue to enforce securities fraud in the United States.[53] Courts have started to retreat from this position, though, and now are more hesitant to find an implied private right of action.[54]

---

48 *Id.*

49 Marbury v. Madison, 5 U.S. 137, 163 (1803) (citing Blackstone's Commentaries).

50 *Id.* at 163.

51 William F. Schneider, *Implying Private Rights and Remedies under the Federal Securities Act*, NORTH CAROLINA LAW REVIEW, vol. 62, ser. 5, 1 June 1984, 853–903, 855.

52 *Id.*

53 Kevin Outterson, *No right without a remedy,* INCIDENTAL ECONOMIST (May 31, 2011, 10:04 AM), http://theincidentaleconomist.com/wordpress/no-right-without-a-remedy/.

54 *See* Cort v. Ash, 422 U.S. 66 (1975) (creating a four-part test to determine whether a private right of action was implied, one part of which was congressional intent); *see also* Touche Ross

It is necessary to enact federal legislation to protect the most valuable and sensitive information we possess. Congress should enact national standards that provide fundamental privacy rights for patients and define responsibilities for those who serve them. As it stands now, if a healthcare provider violates the HIPAA Privacy Rules, the Office for Civil Rights of HHS may investigate and impose civil and criminal penalties against the violating healthcare provider.[55] As stated above, HIPAA does not provide a private cause of action to individuals affected by a healthcare privacy breach.[56] An individual whose private health information has been used or disclosed by a healthcare provider in violation of HIPAA's privacy rules may not bring a civil claim against the health care provider under HIPAA.[57]

HIPAA explicitly preempts any contrary provision of state law, meaning that a state law claim cannot be brought where a healthcare provider cannot comply with both the state and federal laws, or where the state law is an impediment to HIPAA's objectives.[58] Past decisions by state courts, however, have held that HIPAA is the standard industry practice for healthcare providers and may form the basis for state law negligence claims involving disclosure of patient medical records.[59]

Numerous analyses over the course of several years, produced by government, industry, and professional groups, have identified significant gaps in the protection of our private health information,

---

& Co. v. Redington, 442 U.S. 560, 575 (1979) (calling congressional intent the "central inquiry").

55 45 CFR § 160.312 (2006).

56 OFF. OF THE ASSISTANT SEC'Y FOR PLANNING & EVALUATION, CONFIDENTIALITY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION, *supra* note 40.

57 Edward Vishnevetsky, *Can A HIPAA Violation Give Rise to a Private Cause of Action?*, HEALTHCARE DAILY MAG. (May 28, 2014), http://healthcare.dmagazine.com/2014/05/27/can-a-hipaa-violation-give-rise-to-a-private-cause-of-action/.

58 OFF. OF CIVIL RIGHTS, U.S. DEP'T OF HEALTH AND HUMAN SERVICES, *Does the HIPAA Privacy Rule Preempt State Laws?* HHS.GOV, (Dec. 18, 2015), www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html.

59 Ten state courts (Connecticut, Delaware, Kentucky, Maine, Minnesota, Montana, North Carolina, Tennessee, Utah and West Virginia) have looked to HIPAA to evaluate the relevant standard of care. The Connecticut Supreme Court was the first to actually declare that HIPAA establishes a standard of care. *See* David Harlow, *HIPAA: Liability to private parties for violations,* MEDCITYNEWS.COM (Nov. 16, 2014), https://medcitynews.com/2014/11/hipaa-liability-private-parties-violations/.

especially in the form of unregulated data exchange.[60] The National Committee on Vital and Health Statistics held hearings and advised on this issue. After six days of hearing witnesses from the full spectrum of public and private communities, concerned with privacy, consumer interests, and operation of the healthcare system, the Committee strongly recommended that the 105th Congress enact a health privacy law. [61] The Office of Technology Assessment conducted a study of privacy and medical information, which noted that the absence of legislation "allows for a proliferation of private sector computer databases and data exchanges without regulation, statutory guidance, or recourse for persons wronged by abuse of data."[62]

These various groups have recommended federal legislation to close these gaps.[63] Further, the fact that Congress, in HIPAA, mandated that HHS produce these recommendations is evidence that Congress recognizes that the time has come for action.

CURRENT PATIENT REDRESSABILITY UNDER HIPAA

Under the current HIPAA framework, if a covered entity improperly discloses a patient's protected health information, the events that follow are slightly counterintuitive. Though a wronged-patient can file a complaint with the Office of Civil Rights (OCR), a sub-entity of HHS, doing so is not a method by which the wronged-patient can seek personal redress.[64]

---

60 Standards for Privacy, *supra* at note 20.

61 The National Committee on Vital and Health Statistics is an advisory committee to the Secretary of Health and Human Services. It was established by the Public Health Service Act § 306(k), 42 U.S.C. § 242k(k), and its membership was expanded to include persons distinguished in "privacy and security of electronic information" by HIPAA. In the course of its consultation, the Subcommittee on Privacy and Confidentiality held six days of hearings on health privacy during the first two months of 1997. Witnesses included healthcare providers, researchers, public health authorities, Federal and State oversight agencies, accreditation organizations, insurers, claims processors, pharmaceutical manufacturers, Federal agencies, law enforcement agencies, and patient and privacy advocates.

62 OFF. OF TECH. ASSESSMENT, U.S. CONGRESS, OTA-TCT-576, *Protecting Privacy in Computerized Medical Information* (1993).

63 *Id.*

64 *Id.*

Once a patient learns of the covered entity's HIPAA violation (or HIPAA non-compliance), the patient must file a complaint with OCR.[65] OCR then enforces HIPAA's privacy and security rules by investigating complaints and performing compliance reviews.[66] After reviewing all the information gathered, OCR will determine that the covered entity either did or did not violate the requirements of the Privacy and Security Rules.[67] In the case of noncompliance, OCR attempts to resolve the case with the covered entity by obtaining voluntary compliance, corrective action, and a resolution agreement.[68] Failure to comply with HIPAA can also result in civil and criminal penalties; however, those penalties are not paid to the wronged-patient but rather (inexplicably) to HHS. If the complaint is that an action is a violation of the criminal provision of HIPAA, OCR refers the complaint to the Department of Justice (DOJ) for investigation.[69]

If a covered entity does not satisfactorily resolve the matter, OCR may decide to impose civil money penalties on the covered entity.[70] These penalties are determined based on a tiered civil penalty structure.[71] The secretary of HHS has discretion in determining the amount of the penalty, based on the nature and extent of the violation, and the nature and extent of the harm resulting from the violation.[72] The secretary is prohibited from imposing civil penalties if the violation is corrected within 30 days. However, this time period may be extended at HHS' discretion.[73] The prohibition from imposing civil penalties is lifted, though, in cases of willful neglect.[74]

---

65 OFF. FOR CIVIL RIGHTS. U.S. DEP'T OF HEALTH AND HUMAN SERVICES, *Filing a HIPAA Complaint*. HHS.GOV (June 16, 2017), https://www.hhs.gov/hipaa/filing-a-complaint/index.html.

66 *HIPAA Violations & Enforcement*, AM. MED. ASS'N, www.ama-assn.org/practice-management/hipaa-violations-enforcement (last visited Feb. 27, 2018).

67 *Id.*

68 *Id.*

69 *Id.*

70 *Id.*

71 *Id.*

72 *Id.*

73 *Id.*

74 *Id.*

For an "unknowing" HIPAA violation, the minimum penalty is $100 per violation, with an annual maximum of $25,000 for repeat violations.[75] The maximum penalty of any HIPAA violation is $50,000 per violation, with an annual maximum of $1.5 million.[76] A "reasonable cause" violation carries a minimum penalty of $1,000 per violation, with an annual maximum of $100,000 for repeat violations.[77] In cases of violations due to willful neglect where the violation or non-compliance is corrected within the time period, the minimum penalty is $10,000 per violation, with an annual maximum of $1,500,000 for repeat violations.[78] The minimum penalty for instances of willful neglect, where the covered entity fails to correct within the time period, is $50,000 per violation, with an annual maximum of $1.5 million; the maximum penalty for any HIPAA violation.[79]

As with the HIPAA civil penalties, there are different levels of severity for criminal violations.[80] Covered entities and specified individuals who "knowingly" obtain or disclose individually identifiable health information, in violation of the Administrative Simplification Regulations, can face a fine of up to $50,000, as well as up to one year imprisonment.[81] Offenses committed under false pretenses increase the maximum penalties to a $100,000 fine and 5 years in prison.[82] Finally, offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, permit fines of up to $250,000 and imprisonment for up to 10 years.[83]

---

75 *Id.*

76 *Id.*

77 *Id.*

78 *Id.*

79 AMERICAN MED. ASS'N, *supra* note 66.

80 *Filing a HIPAA Complaint*, *supra* note 65.

81 *Id.*

82 *Id.*

83 *Id.*

WHAT FEDERAL LEGISLATION PROTECTING PATIENTS' PRIVATE HEALTH INFORMATION WOULD PROVIDE

To effectively protect patients' private health information, a federal privacy law would need to impose new restrictions on those who pay for and provide care, as well as on those who receive information from providers.[84] It should prohibit the disclosure of information that can be used to identify the patient—unless such disclosure is authorized by the patient or as explicitly permitted by the legislation. Disclosures of identifiable information should be limited to the minimum level of disclosure necessary to accomplish the purpose of the disclosure. Such disclosures should only be used for the purposes for which the information was collected within the organization.[85] Consumers should be granted the right to be informed of how their health information is used, and to whom it is disclosed.[86] Providers and payers should maintain a history of disclosures, and those histories should be made accessible to patients. Providers and payers should be required to notify patients in writing of their information practices, including how they store information and what security practices are used to protect their data. Patients should have access to their records, be able to obtain copies, and if necessary, propose corrections to misinformation in their medical records. Additionally, the legislation needs to provide a basis for punishment for those who misuse personal health information and a private right of action so the people who are harmed by misuse may seek redress.[87] There should be criminal penalties for using deception to obtain health information and for violating the Federal Privacy law by knowingly disclosing or misusing medical information. If an individual's rights under the law are violated, he or she should be permitted to bring an action for damages and equitable relief personally. A framework already exists under HIPAA whereby individuals could be compensated for improper disclosures of their private health

---

84 U.S. DEP'T OF HEALTH & HUMAN SERVICES, *Confidentiality of Individually Identifiable Health Information* 2 (1997), https://aspe.hhs.gov/report/confidentiality-individually-identifiable-health-information.

85 *Id.*

86 *Id.*

87 *Id.* at 6.

information vis-a-vis the civil money penalties imposed for non-compliance. However, Congress must act to provide individuals with a private right of action under a federal statute and, puzzlingly, Congress has refused to do so.