Medical Information as a Hot Commodity: The Need for Stronger Protection of Patient Health Information

N. NINA ZIVANOVIC*

INTRODUCTION

Medical data has always demanded more privacy protection because of its personal nature, as well as its value. Employers, insurance companies, pharmaceutical data mining companies, drug manufacturers, and medical researchers all want access to medical information regarding patients' medical histories, diagnoses, prognoses, and treatments.[1] These entities seek medical information to conduct research, assist treatment, provide coverage, assess opportunities, process claims, and market products.[2] Current law governing patient medical information allows certain entities to access this information, and even allows data miners to sell or license prescription information to drug manufactures and advertisers for a profit.[3]

The Health Insurance Portability and Accessibility Act (HIPAA)[4] regulations provide some protection for medical data that is personally identifiable,[5] but fails to protect de-identified data.[6] Data re-identification is the process of matching various fragments of a person's information to deduce that person's identity.[7] Studies

---

* J.D. 2014, University of San Francisco School of Law; B.A. English Literature 2009, California State University, Northridge. The Author wishes to extend her deep appreciation to University of San Francisco School of Law Professor, Susan Freiwald, for her invaluable guidance and assistance on prior drafts. The Author further wishes to thank her parents and brothers for their constant support and encouragement.

1. *See* Christopher R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information*, 36 VT. L. REV. 931, 933 (2012).

2. *Id.*

3. Jennifer L. Klocke, *Prescription Records for Sale: Privacy and Free Speech Issues Arising From the Sale of De-Identified Medical Data*, 44 IDAHO L. REV. 511, 512 (2008).

4. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1938 (1996).

5. "Protected health information under HIPAA is *individually identifiable* health information. *Identifiable* refers not only to data that is explicitly linked to a particular individual .... It also includes health information with data items which reasonably could be expected to allow individual information." *See De-Identified Health Information (HIPAA)*, UNIV. OF MIAMI, http://privacy.med.miami.edu/glossary/xd_deidentified_health_info.htm (last visited Apr. 24, 2015) (providing a list of potential identifiers).

6. *See* Smith, *supra* note 1, at 935; *see also De-Identified Health Information (HIPAA)*, *supra* note 5 ("[I]nformation is considered de-identified if [the listed potential identifiers] have been removed, *and* there is no reasonable basis to believe that the remaining information could be used to identify a person.").

7. *Re-Identifcation*, ELEC. INFO. PRIVACY CENTER,

indicate that de-identified information is no longer as safe from re-identification as the U.S. Department of Health and Human Services (HHS) thought when it created the HIPAA Privacy Rule.[8] Furthermore, scholarship indicates that the regulations currently governing the privacy of personal health information are far from ironclad.[9] Businesses manage to circumvent the law by colluding with other companies to share medical information, shielding themselves from HIPAA liability.[10] Under HIPAA, if entities combine into one covered entity, they may also combine their medical information, thus evading the HIPAA limitations on how and with whom personal medical information can be shared.[11] HIPAA's regulations apply to "covered entities," that include healthcare providers, healthcare clearinghouses, and health plans.[12] These entities obtain medical care payments from both private and government sources,[13] such as Medicaid and Medicare.

Almost every person in the world is linked to at least one fact in a computer database.[14] Thus, it is possible for pharmaceutical companies and insurance companies to re-identify data by combining de-identified medical data with information from public databases. The loopholes in the law, along with the ability to re-identify data, undermine the efficacy of HIPAA's Privacy Rule. Without stricter regulation on the dissemination of medical data, anyone including employers, insurance companies, or even stalkers, can obtain an individual's personal medical information for nefarious uses such as blackmail, harassment, discrimination, or to commit financial or identity theft.

Additionally, HIPAA fails to effectively protect psychotherapy notes.[15] The psychotherapy provision demands that psychotherapists separate psychotherapy notes from medical notes to provide greater protection over the use and distribution of psychotherapy notes.[16]

---

https://epic.org/privacy/reidentification/ (last visited Mar. 2, 2015).

8. HIPAA Privacy Rule, 45 C.F.R. pts. 160, 164 (2015). *See also* Pal Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706 (2010).

9. *See* Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 306 (2003) ("[G]overnment digital surveillance and monitoring blurs the line between physical and informational privacy. Many of the privacy harms fall through the cracks . . . and the ubiquity of personal information in the digital age and its use by private parties causes problems that the current discrete legal regime cannot control.").

10. Smith, *supra* note 1, at 938.

11. *Id.*

12. Sean T. McLaughlin, *Pandora's Box: Can HIPAA Still Protect Patient Privacy Under a National Health Care Information Network*, 42 GONZ. L. REV. 29, 40 (2006).

13. *Id.* at 40–41.

14. *See* Ohm, *supra* note 8, at 1748.

15. *See* Stephanie O. Corley, *Protection for Psychotherapy Notes Under the HIPAA Privacy Rule: As Private As A Hospital Gown*, 22 HEALTH MATRIX 489, 491–92 (2013); 45 C.F.R. § 164.510 (2015).

16. *See* 45 C.F.R § 164.501 (2015).

However, a major weakness to this psychotherapy provision is that HIPAA vaguely defines psychotherapy notes, which gives psychotherapists the discretion to document notes as either psychotherapy or medical. If psychotherapists choose to document everything in a patient's medical notes, that information will only receive the basic HIPAA protection rather than the stronger psychotherapy notes protection.[17]

Congress and the HHS must update HIPAA to better regulate de-identified information, close the loopholes that encourage evasive business practices, and prevent disclosures of psychotherapy notes in general medical records.

This Article discusses the inadequacy of HIPAA regulations in protecting the privacy of medical data, and argues that the HHS should give patients a choice in how their medical information is used once the patient leaves the doctor's office. Part I discusses the foundation of health privacy, including the original principles behind HIPAA and the political conflicts that led to the enactment of the current version of HIPAA. Part II concedes that by enacting the Health Information Technology for Economic and Clinical Health (HITECH) Act[18] Congress developed new safeguards to protect medical information, but explains lawmakers still must further update HIPAA. Part III provides background on the importance of protecting identifiable and de-identified patient health information, further examines the lax protection of de-identified patient health information, and proposes new laws to regulate de-identified data. Part IV examines the loopholes in the existing regulations and argues that HHS should close these loopholes. This Article concludes that Congress must update the laws protecting medical information to reflect contemporary expectations of privacy while also taking into consideration modern data re-identification techniques and abilities.

I. THE INITIAL PRINCIPLES BEHIND THE ENACTMENT OF HIPAA

Prior to HIPAA, state law and common law protected the right to privacy of medical data.[19] However, the lack of uniformity among state law presented a problem for consumers and healthcare providers as the scope of the healthcare industry expanded.[20] In 1996, Congress responded by enacting HIPAA, and also self-imposed a deadline of August 21, 1999 to pass health information privacy

17. Corley, *supra* note 15, at 491–92.

18. The Health Information Technology for Economic and Clinical Health Act is Title VIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, 226–79 (2009) (codified in various sections of 42 U.S.C.).

19. Edward J. Markey, *POLICY ESSAY: Commerce with a Conscience: Balancing Privacy and Profit in a Digital World*, 41 HARV. J. ON LEGIS. 377, 380 (2004).

20. *Id.*

legislation through the Act.[21] Congress failed to meet this deadline, and, as indicated in HIPAA, the burden of proposing privacy regulations passed to the HHS and President Clinton.[22]

During the rule-making period, approximately 52,000 public comments poured into the HHS discussing the need for a balance between privacy and commerce.[23] According to Shailagh Murray of the *Wall Street Journal*, criticism from privacy advocates and civil libertarians arguing for greater restraint grew when the Clinton administration contemplated granting more tolerance for law enforcement seeking personally identifiable information.[24] The HHS and the Clinton Administration responded by proposing strict regulations that would require patient consent or approval from a review board before healthcare entities could use an individual patient's health information for healthcare treatment, payment, and operations, thus making personally identifiable information less accessible.[25]

The Clinton Administration's proposed privacy rule provided a patient with the power to withhold consent in disclosing personal health information for most routine purposes.[26] It defined routine purposes as "treatment, payment and health care operations," which broadened the scope of protection to the most common types of uses and disclosures of medical information.[27]

However, when President Bush took office, he scaled back the regulations.[28] Health privacy advocates disfavored the Bush Administration's amendment that replaced the former requirement of a patient's consent with merely requiring notifications of how the medical information is used and disclosed.[29] Critics of the amendments responded by introducing bills to strengthen the privacy laws.[30] For example, in 2003, Representative Edward J. Markey introduced the Stop Taking Our Health Privacy Act (the "STOHP Act"), which focused mainly on strengthening patient consent requirements and restricting pharmaceutical marketing.[31]

---

21. Catherine Louisa Glenn, *Protecting Health Information Privacy: The Case For Self-Regulation of Electronically Held Medical Records*, 53 VAND. L. REV. 1605, 1610 (2000).

22. *Id.*

23. Markey, *supra* note 19, at 381.

24. Shailagh Murray, *White House Seeks Compromise On Access to Health Information*, WALL ST. J., Oct. 25, 1999, at A4 (arguing that federal law, 18 U.S.C. § 2710, imposes stricter privacy regulations on video-rental records, requiring consent for the release of personally identifiable data, than it does for health information).

25. Glenn, *supra* note 21, at 1610.

26. *See* Markey, *supra* note 19, at 382–83.

27. *Id.*

28. Ralph Ruebner & Leslie Ann Reis, *Hippocrates to HIPAA: A Foundation for a Federal Physician-Patient Privilege*, 77 TEMP. L. REV. 505, 567–68 (2004).

29. Markey, *supra* note 19, at 382.

30. *See id.* at 385–86.

31. Stop Taking Our Health Privacy Act, H.R. 1709, 108th Cong. (2003).

Unfortunately, Congress failed to act on Representative Markey's bill.[32]

II. CONTEMPORARY RESEARCH INDICATES A NEED TO REEVALUATE HIPAA

Years after the enactment of HIPAA, Congress passed another law governing the protection of health information, known as the HITECH Act, in response to the movement to transfer all medical or health records into electronic form.[33] President Bush strongly supported the adoption of electronic records, as did President Obama, who called for a nationwide interconnected network of medical data in electronic form to be implemented by 2014.[34] In fact, there is evidence that the government might begin imposing penalties on entities that do not keep their medical records in electronic format.[35]

The use of electronic medical records instead of handwritten documents yields many benefits.[36] For example, electronic records are clear and legible, which reduces the risk that a doctor or nurse will misread a patient's records, reducing the harms caused by human error.[37] Electronic records also assist in the organization of documents because they are easier to maintain and require less storage space.[38]

Despite the benefits of electronic storage, once patient data is entered electronically, medical practitioners and patients lose an element of control over the information and more entities have access to it.[39] Congress expanded the definition of covered entities in the HITECH Act, thereby extending the reach of HIPAA to include business associates.[40] The HITECH Act defines business associates as persons and organizations that perform functions or activities for or on behalf of covered entities that involve the use or disclosure of patient health information.[41]

Although Congress enacted HIPAA and the HITECH Act to

---

32. *Id.*

33. Katherine Drabiak-Syed, *Granular Control of EHRS to Overcome Fragmented Disclosure Law: How Policy Choices for Granularity Will Affect Clinical Care, Impact Secondary Use of Health Information, and Alter Risks for Patients and Providers*, 10 IND. HEALTH L. REV. 39, 45 (2013).

34. *See* Corley, *supra* note 15, at 505–06.

35. *Id.* at 506.

36. Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 683 (2007).

37. *Id.*

38. *See* Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and the Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1444 (2002).

39. Terry & Francis, *supra* note 36, at 683.

40. *See* 45 C.F.R. § 160.103 (2015).

41. *Id.*

increase federal protection of medical information, privacy breaches of medical data persist. The HHS reported that in 2010, Georgetown University Hospital, NYU Hospital Center, the University of California San Francisco, and the University of Florida all fell victim to medical data breaches.[42] A former employee of the University of California Los Angeles (UCLA) was found guilty of accessing UCLA medical records 323 times during a three-week period.[43] The employee was allegedly searching the database to find celebrities' medical records.[44] In 2008, another UCLA employee sold medical records to tabloids, targeting celebrities like Britney Spears and Farrah Fawcett.[45]

No statutory framework for protecting medical records can completely prevent privacy breaches while simultaneously allowing medical entities virtual access. Any access inherently opens the system to vulnerabilities. However, the laws must be kept up-to-date. HIPAA and the HITECH Act fail to address the issues concerning de-identified data. According to Professor Paul Ohm, the technique of de-identifying information to render it anonymized worked well a decade ago, but recent studies show it is now much easier to re-identify data.[46] As the health industry grows, and more entities fall under HIPAA's definition of covered entity or the HITECH Act's definition of business associate, many more entities will have access personal health information.[47] HIPAA allows both covered entities and business associates to freely share information among each other.[48] As Professor Ohm suggests, lawmakers must revisit patient health information laws in light of technological advancements that undermine patient privacy.[49]

III. PRIVACY PROTECTION OF IDENTIFIABLE AND DE-IDENTIFIED PATIENT HEALTH INFORMATION

42. Vadim Schick, *After HITECH: HIPAA Revisions Mandate Stronger Privacy and Security Safeguards*, 37 J.C. & U.L. 403, 404–05 (2011) (noting that the Department of Education has indicated that colleges and universities are among the most vulnerable to privacy breaches because they contain records that are similar to bank records, yet easier to access).

43. Bill French, *Former UCLA Healthcare Worker Sentenced to Prison for Snooping*, NBC L.A. (Apr. 28, 2010), http://www.nbclosangeles.com/news/local/Former-UCLA-Healthcare-Worker-Sentenced-Prison-Snooping-92265634.html.

44. *Id.*

45. Schick, *supra* note 42, at 421.

46. Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33, 39 (2010) (describing how Ohm provides instances where information that was considered de-identifed was ultimately found to be re-identified, including when researchers were able to re-identify people with movie ratings after a Netflix contest).

47. 45 C.F.R. § 160.103 (2015).

48. Schick, *supra* note 42, at 412.

49. Ohm, *supra* note 8, at 1706.

A. NO LEGAL PROTECTIONS FOR DE-IDENTIFIED DATA

Neither the U.S. Supreme Court nor the HHS regulate the manner in which entities use and disclose patient health information.[50] Federal privacy laws "do not restrict access, use, or disclosure of non-identifiable data."[51] However, the HHS provides specific guidelines in the HIPAA Privacy Rule on what information must be removed and rendered de-identified from patient health information.[52] Such information includes patient names, addresses, phone numbers and social security numbers, as well as unspecified unique identifiers.[53] Medical personnel use computer programs to strip personal health information of identifiers so that it no longer falls under HIPAA regulation to ensure compliance with the regulations.[54]

Select state legislation shows a heightened concern for how and to who covered entities are sharing and selling medical data.[55] Despite having HIPAA, some states continued to enact more stringent privacy laws, which suggests HIPAA does not provide adequate protection.[56] For example, states such as New Hampshire, Maine, and Vermont, passed laws prohibiting the sale of pharmaceutical information to third parties—i.e., data miners and drug manufacturers.[57] However, the states' statutes protected prescriber information instead of patient information, and the Supreme Court struck them down on First Amendment grounds.[58] In *Sorrell v. IMS Health Inc.*, the Supreme Court struck down Vermont's law (which rendered the New Hampshire and Maine statutes moot) holding that the state's justifications for enacting the law were insufficient to overcome its content-based discrimination.[59] Nevertheless, the Court acknowledged "the capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal

50. *See* Beverly Cohen, *Regulating Data Mining Post-Sorrell: Using HIPAA to Restrict Marketing Uses of Patients' Private Medical Information*, 47 WAKE FOREST L. REV. 1141, 1159–60 (2013); Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

51. Lawrence O. Gostin, James G. Hodge, Jr. & Lauren Marks, *The Nationalization of Health Information Privacy Protections*, 37 TORT & INS. L.J. 1113, 1124 (2002).

52. *See* 45 C.F.R. § 164.514 (2015).

53. *Id.*

54. Cohen, *supra* note 50, at 1163.

55. *See* David Orentlicher, *Prescription Data Mining and the Protection of Patients' Interests*, 38 J.L. MED. & ETHICS 74, 78 (2010).

56. *Id.*

57. C. Christine Porter, *Constitutional and Regulatory: De-identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information*, 5 SHIDLER J.L. COM. & TECH. 3, 7 (2008) ("Federal district courts in Maine and New Hampshire have struck down recently-enacted privacy laws on First Amendment grounds.").

58. Smith, *supra* note 1, at 967–68.

59. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2672 (2011).

privacy and the dignity it seeks to secure."[60]

B. THE IMPORTANCE OF PROTECTING PATIENT HEALTH INFORMATION

Two principles underlie the need for increased protection of patient health information—(1) health data is inherently personal; and (2) the shift from paper to electronic records makes the information susceptible to a data breach, providing access to private medical data to anyone who is technologically savvy.[61] Privacy breaches place medical information at risk for unwarranted and detrimental disclosure.[62] Victims of leaked medical information could face discrimination in social circles, the workplace, and from insurance companies due to the social stigma associated with physical and mental ailments.[63] Such unwarranted disclosures also risks patients losing trust in medical providers' ability to maintain confidentiality.[64]

People often feel stress and embarrassment when their private medical information is disseminated without their consent.[65] Surveys show that 67% of Americans are concerned with the privacy practices regarding their health information.[66] Of the patients who belong to ethnic and racial minorities, 73% expressed fear that their medical information is not adequately protected.[67] A similar survey indicated that patients felt that all medical information deserved the same level of protection regardless of what the record reveals.[68]

When medical information is recorded, the lack of control over what is circulated and to whom it is disseminated has been described as dehumanizing healthcare.[69] Patients disclose intimate details of their past and present medical history to trusted institutions with an expectation of privacy.[70]

C. THE NEED FOR STRONGER PROTECTION OF DE-IDENTIFIED PATIENT HEALTH INFORMATION

De-identified data contains sensitive information that can be re-

60. *Id.*

61. Gostin et al., *supra* note 51, at 1114.

62. Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 489 (1995).

63. Ruebner & Reis, *supra* note 28, at 548.

64. Gostin et al., *supra* note 51, at 1114.

65. *See* Smith, *supra* note 1, at 936.

66. Terry & Francis, *supra* note 36, at 696.

67. *Id.*

68. *Id.* at 697.

69. DeVries, *supra* note 9, at 298.

70. Parkson v. Cent. DuPage Hosp., 435 N.E.2d 140, 143 (Ill. App. Ct. 1982) (holding that hospitals were not required to release medical information of patients not party to the suit because it is privileged).

identified.[71] Even if de-identified, patient health information still contains intimate details about a person's life and health, such as whether a woman previously had an abortion or whether one has a sexually transmitted disease, thus patients have a legitimate interest in its protection.[72] Advances in re-identification techniques continue to expose the fallacy that de-identified data is untraceable.[73] De-identified data may be relatively safe from re-identification when examined in isolation, but computer scientists have and continue to discover ways to re-identify data by combining various de-identified data pieces with public information.[74] By looking at specific or rare characteristics of a person, computer scientists can connect the dots to successfully re-identify.[75] As data mining algorithms continue to improve, datasets transform information that was once thought to be non-identifying into personal identifying information.[76]

In *Northwestern Memorial Hospital v. Ashcroft*,[77] Judge Posner recognized that even after personal information is de-identified, savvy researchers, or acquaintances with sufficient information about a person, might be able to make enough inferences to identify the person.[78] In some contexts successful re-identifications could expose patients to discrimination or ridicule.[79]

Re-identification presents the possibility of serious privacy breaches that are essentially irreversible.[80] A person's identity becomes linked to his or her "anonymous virtual identity," which increases the likelihood of future privacy breaches.[81] For instance, "[if] a Netflix subscriber's rankings were re-identified . . . then that person can never again disclose any information about her movie viewing, because it can then be traced back to her real identity."[82] Allowing entities to use de-identified data solely to promote medical research and breakthroughs is ideal in theory, but unrealistic in practice.[83] When information is released on any sort of database, as nearly all medical information is today, it cannot be recaptured.

---

71. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1847 (2011).

72. Smith, *supra* note 1, at 982.

73. Ohm, *supra* note 8, at 1704.

74. Schwartz & Solove, *supra* note 71, at 1841.

75. *Id.* at 1824.

76. Klocke, *supra* note 3, at 520.

77. 362 F.3d 923 (7th Cir. 2004).

78. Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117, 1156–57 (2013).

79. *See* DeVries, *supra* note 9, at 303.

80. *See* Ohm, *supra* note 8, at 1705 ("Every successful re-identification, even one that reveals seemingly non-sensitive data like movie ratings, abets future re-identification.").

81. *Id.*

82. Porter, *supra* note 57, at 12.

83. *See* Schwartz & Solove, *supra* note 71, at 1847.

D. UNDER HIPAA THIRD-PARTY RECIPIENTS OF MEDICAL INFORMATION ARE NOT REQUIRED TO PROTECT IT

HIPAA does not prevent covered entities from selling or giving de-identified information to third parties such as data miners, drug manufacturers, and research institutions.[84] This exacerbates the risk of only relying on de-identification techniques for protecting data. The company that sells the data may have a strict internal privacy policy regarding the protection of data; but the data purchaser may not, and proceed to re-identify the patient's private data.[85] Even when a company claims to maintain a strict data privacy policy, it may choose to weaken its privacy policy when pressed financially or even sell the data to parties that might have weak or non-existent privacy policies.[86]

Confidentiality is an even greater issue once covered entities sell the data to third parties who do not owe a duty to patients under HIPAA.[87] A 1993 privacy survey revealed that over 60% of Americans felt that hospitals, researchers, and pharmaceutical companies should be required to obtain patient permission before using medical information, even if the information contains no patient health information as defined by HIPAA.[88] Absent a regulatory framework that protects the information that covered entities sell to third parties, patients will have no recourse in the event of a privacy breach since the third-party buyers do not legally owe the same duty of confidentiality to patients as covered entities.[89]

E. PROPOSAL TO PROTECT DE-IDENTIFIED DATA

Lawmakers must update regulations to address current privacy threats and protect de-identified medical data.[90]

1. Patient Autonomy

One possible solution to protect patient health information would be to enact laws that empower individual patients to decide whether to share their de-identified medical information.[91] Lawmakers could grant patients the choice to opt-out of sharing, limit when and to whom their data is shared, or allow unrestricted

84. Smith, *supra* note 1, at 973.

85. Porter, *supra* note 57, at 17.

86. *Id.* at 19 (discussing how Toysmart, an internet-only retailer, originally had a very strict privacy policy which it relaxed in order to sell its consumer information when it faced the possibility of bankruptcy).

87. Smith, *supra* note 1, at 973.

88. Sharon R. Schwabel, *Are You Taking Any Prescription Medication? A Case Comment on* Weld v. CVS Pharmacy, Inc., 35 NEW ENG. L. REV. 909, 923–24 (2001).

89. *Id.* at 961.

90. Smith, *supra* note 1, at 982.

91. *Id.* at 948–49.

sharing.[92] An effective solution would be to provide patients with a proactive approach, rather than the current reactive approach, which does "not empower patients to prevent unauthorized access to their prescription [patient health information] but only allow them to file suit once a breach of privacy occurs."[93]

2. Create Laws to Protect De-identified Data

If lawmakers consider requiring covered entities to receive individual patient consent too burdensome, Congress should increase the statutory protection of de-identified data. California is one of few states that strengthened its health privacy laws above HIPAA's threshold.[94] California's Health Information Exchange Practice Principles state "[d]e-identified individual health information shall not be re-identified unless specified by law."[95] The law provides that if the de-identified individual health information is re-identified, it becomes subject to the provisions in the law governing protection of personally identifiable information.[96] Additionally, the law prohibits the disclosure of de-identified information if there is a reasonable basis to believe that it can be used to identify an individual.[97]

Other laws that protect personal information should also guide legislation to protect medical information. For example, the Children's Online Privacy Protection Act (COPPA)[98] governs the information commercial websites obtain from minors under the age of thirteen.[99] COPPA requires entities to (1) obtain prior parental consent before collecting online information from a minor; (2) implement privacy policies disclosing its information-collection practices, specifying the types of information collected and how it is used; and (3) obtain prior parental consent before using or disclosing the collected personal information.[100] Medical information warrants similar privacy protections.

Lawmakers might oppose legislation to increase privacy protection of de-identified medical information for fear of limiting the amount of shared information that is beneficial to society.[101] For example, personal medical information may be used for healthcare research, for "care management educational communications provided to patients on such matters as treatment options," and for

92. *See* Terry & Francis, *supra* note 36, at 725.

93. Smith, *supra* note 1, at 984.

94. *See* CAL. CODE REGS. tit. 22, § 126030 (2015).

95. *Id.*

96. *Id.*

97. *Id.*

98. 15 U.S.C. §§ 6501–06 (2012).

99. Patricia Sanchez Abril & Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights*, 6 NW. J. TECH. & INTELL. PROP. 244, 258 (2008).

100. *Id.*

101. Ohm, *supra* note 8, at 1770.

education programs designed to provide doctors and other medical personnel with information.[102] Nevertheless, a hybrid of California's law and COPPA may better protect medical information while still allowing for the flow of information to medical researchers.

IV. LOOPHOLES IN HIPAA REGULATIONS

Covered entities and third parties easily access personal medical information due to loopholes in HIPAA regulations. Businesses such as pharmaceutical companies, large drugstore chains, and insurance companies benefit from identifying patient medical information because it provides them with useful marketing information to identify potential consumers.[103] Regulations must be enacted to strengthen privacy protection of information that is shared between entities and also in psychotherapy notes.

A. SHARING INFORMATION AMONG COVERED ENTITIES IS LESS REGULATED

Covered entities avoid liability under HIPAA and freely share information with non-covered entities by merging the two into a single entity. Under HIPAA, covered entities can freely share personally identifiable patient information with one another as long as they establish they are one entity.[104] The HIPAA Privacy Rule permits covered entities to use and share patient health information with each other for "treatment, payment, or healthcare operations."[105] HIPAA allows covered entities to access medical information that contains personal information about a patient's mental and physical health as well as information about a patient's social behavior, personal relationships, and financial status.[106] The Privacy Rule states that healthcare providers such as doctors, or clinics, are considered a covered entity if they "transmit any health information in electronic form in connection with a transaction covered by [the regulation]."[107] Additionally, covered entities include business associates such as lawyers, billing companies, and accountants.[108] The definition of business associates includes any person or company whose work includes the "use or disclosure of individually identifiable health information."[109]

---

102. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2660 (2011).

103. *See* IMS Health Inc. v. Mills, 616 F.3d 7, 16 (1st Cir. 2010).

104. *See* Smith, *supra* note 1, at 938.

105. 45 C.F.R. § 164.508(a)(2)(i) (2015); *see also* 45 C.F.R. § 164.512(2015) (providing uses and disclosures for which an authorization or opportunity to agree or object is not required).

106. *See* Gostin, *supra* note 62, at 490 (describing that health records contain a vast amount of personal information with multiple uses).

107. *HIPAA Guidance—Use of Protected Health Information in Human Subjects Research at UNT*, UNT RESEARCH & ECON. DEV., http://research.unt.edu/hippa-guidance (last visited Apr. 24, 2015).

108. *See* Cohen, *supra* note 50, at 1161.

109. 45 C.F.R. § 160.103 (2015).

Merging entities can circumvent the HIPAA regulations, and the law is subject to abuse by powerful companies with financial interests in medical health information.[110] HIPAA does not prohibit covered entities from merging with non-covered entities to form one single unit for the purposes of sharing patient health information.[111] The merger allows a non-covered entity to access sensitive medical information that it did not have prior to the merger.

For example, CVS Pharmacy took advantage of this loophole when it merged with the pharmacy benefits manager Caremark in 2007.[112] Generally, pharmacy benefits managers are not considered covered entities under HIPAA.[113] CVS Caremark, the newly merged company, considered itself "an affiliated group of pharmacies that is treated as a single entity for the purposes of sharing information."[114] In the ongoing lawsuit between Burton's Pharmacy and CVS Caremark, the plaintiffs allege CVS Caremark uses patient health information to "directly target non-CVS patients and solicit their business to CVS-owned retail stores and their purchases of CVS-branded over-the-counter-products."[115] By operating as a single entity, Caremark is permitted to use specific patient characteristics and private patient health information that CVS originally possessed to customize marketing strategies while simultaneously evading HIPAA's privacy policies for covered entities.[116] The plaintiffs cited CVS Caremark's Notice of Privacy Practices and directed attention to the fact that CVS Caremark declared that it was a single entity comprised of affiliated pharmacies to argue that Caremark should also be considered a covered entity under HIPAA.[117] The CVS Caremark Notice of Privacy Practices indicated that CVS could freely share patient information with other associated entities.[118] This case demonstrates the HIPAA Privacy Rule fails to adequately protect personally identifiable information and falls short of prohibiting evasive practices by self-serving covered entities.[119]

B. PROPOSAL TO STRENGTHEN REGULATIONS GOVERNING SHARING OF INFORMATION AMONG COVERED ENTITIES

Covered entities should be required to obtain patient consent

110. *See* Theo Francis, *Spread of Records Stirs Patient Fears of Privacy Erosion*, WALL ST. J. (Dec. 26, 2006), http://www.wsj.com/articles/SB116709136139859229.

111. Smith, *supra* note 1, at 938.

112. *Id.* at 936.

113. *See id.*

114. *Id.* at 938.

115. Complaint, Burton's Pharmacy, Inc. v. CVS Caremark Corp., No. 1:11-cv-2 (M.D.N.C. Jan. 3, 2011).

116. Smith, *supra* note 1, at 937–38.

117. *Id.* at 938.

118. *Id.*

119. *Id.*

prior to using and disclosing patient health information. Congress should revisit the principles behind the Clinton Privacy Rule,[120] and determine whether an amendment to the HIPAA provisions is necessary.[121] The Clinton Privacy Rule gave individuals the right to refuse the use and disclosure of patient health information for most routine purposes.[122]

Congress included a provision in the HITECH Act that requires covered entities to respect an individual's request to not use or disclose personal health information; however, this only pertains to documents of services and procedures for which the patient paid a healthcare provider directly.[123] This rule does not apply to services or procedures where providers were paid by a health maintenance organization.[124] Many patients, not just those who can pay out-of-pocket, may object to the manner in which entities share personally identifiable information. All patients should have a right to protect their personal medical information. Thus, lawmakers should expand the scope of this provision to allow all patients to request nondisclosure of their personal health information, not just the patients who are wealthy enough to pay for treatment out-of-pocket.

1. Transparency

Lack of transparency also causes entities to commit evasive practices, such as in the CVS Caremark situation, while simultaneously complying with HIPAA. Transparency refers to making data processing open and understandable to the affected individual.[125] A patient should be able to track (similar to the way that United Postal Service allows for tracking of shipments) how, when, and why personal information is used or shared to establish accountability.[126]

Maintaining transparency can be difficult when numerous entities obtain and use information. Due to all the different entities

120. *See* Markey, *supra* note 19, at 382.

121. Terry & Francis, *supra* note 36, at 719 (citing a 2005 survey conducted by the Markle Foundation, which found that 70% of respondents indicated that it was a "top" or "high" priority that their electronic medical information be shared only with their consent).

122. *See* Markey, *supra* note 19, at 382–83. This definition was narrowly construed "to establish privacy protections for the most common types of uses and disclosures of health information." *See id.*

123. Schick, *supra* note 42, at 408.

124. *Id.* at 409 (explaining that the personal health information that pertains to services or procedures that were paid for in any way other than out of pocket is governed by the HIPAA; individuals may request that covered entities restrict the use and disclosure of personal health information, but covered entities may refuse these requests). Health maintenance organizations require you to select a primary care provider who is responsible for managing and coordinating all of your health care and receive most or all of your health care from a network provider. *See* Michael Bihari, *HMOs v. PPOs—What are the Differences Between HMOs and PPOs?*, ABOUT HEALTH (Dec. 20, 2014), http://healthinsurance.about.com/od/understandingmanagedcare/a/HMOs_vs_PPOs.htm.

125. *See* Smith, *supra* note 1, at 985–86.

126. Abril & Cava, *supra* note 99, at 272–73.

that obtain access to personal medical information, tracking may overwhelm patients. To remedy this problem, Professors Nicolas P. Terry and Leslie P. Francis proposed the "Circle of Care."[127] The Circle of Care operates as an alternative aid to protect medical information by decreasing the size of the population that can access personal medical data.[128] Terry and Francis define the Circle of Care as those providers within the patient's medical team that may access information on a need-to-know basis.[129] This concept redefines the meaning of covered entities and business associates, creates a safeguard prohibiting entities from taking advantage of the merger loophole, and is less likely to overwhelm patients attempting to track their health data.

2. Destruction of Documents Provision

New regulations governing personal medical information should also consider how long it is necessary for the entities to store the information.[130] In 1988, Congress enacted the Video Privacy Protection Act (VPPA), which protects personally identifiable information of videotape rental consumers.[131] The VPPA requires videotape service providers to "destroy all personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information" from the consumer.[132] Video service providers can also postpone destruction if there is a request from anyone with informed, written consent from the consumer, a government warrant, or pursuant to a court order.[133] Congress should create a similar regulation for medical records to ensure that entities do not retain medical information if the entity has successfully used the information for the purpose gathered. Absent a mandatory destruction policy, fragments of information continue to accumulate, which makes it easier to match those pieces and deduce a person's identity.

C. LOOPHOLES IN THE PRIVACY RULE'S PSYCHOTHERAPY NOTES PROVISION

The Privacy Rule indicates that psychotherapist notes get special protection.[134] Psychotherapy notes are defined as information that is (1) documented by a mental health professional during a private,

127. *See* Terry & Francis, *supra* note 36, at 726–27.

128. *Id.*

129. *Id.*

130. Schwartz & Solove, *supra* note 71, at 1878.

131. 18 U.S.C. § 2710 (2012).

132. *Id.*

133. *Id.*

134. Uses and Disclosures for Which an Authorization is Required. 45 C.F.R. § 164.508 (2015).

group, joint, or family counseling session; and (2) stored separately from the rest of a patient's medical records.[135] Under the provision, the disclosure of a psychotherapist's notes is prohibited absent patient authorization.[136] However, the Privacy Rule grants mental health practitioners deference on how to record notes taken during psychotherapy sessions.[137] In other words, mental health practitioners are not required to separate out psychotherapy notes and can record all information in a general medical chart.[138] When medical personnel combine psychotherapy notes with general medical records the combined information loses special protection under HIPAA.[139]

Patricia Galvin, a San Francisco tax attorney, fell victim to this problem after a serious car accident left her with physical ailments and many medical bills.[140] Galvin's therapist assured her that her psychotherapy notes would remain confidential unless Galvin provided additional authorization to disclose the notes.[141] Galvin released her medical chart to her health insurer in an effort to obtain disability benefits.[142] However, unbeknownst to her, the medical chart contained notes from her psychotherapy sessions, which ultimately led the insurance carrier denying her disability claim.[143] Aside from the rejection of her disability claim, Galvin suffered emotional trauma knowing that her insurance company could so easily gain access to her psychotherapy notes.[144] Galvin stated, "I feel like now I have no privacy.... My most private thoughts, my personal tragedies, secrets about other people, are mere data of a transaction, like a grocery receipt."[145]

HIPAA's broad regulatory language permits "health insurers and medical providers—including doctors, pharmacies, and hospitals—to disclose medical information for treatment, payment and health-care operations, among other situations, without specific patient permission."[146] The HHS indicated covered entities must not share more medical information than is necessary.[147] Yet, it failed to

135. 45 C.F.R. § 164.501 (2015).

136. 45 C.F.R. § 164.508 (2015).

137. *See* Corley, *supra* note 15, at 492. However, there are eight general exceptions to the requirement of patient authorization for disclosure of psychotherapy notes. *See* 45 C.F.R. § 164.508(a)(2) (2015).

138. *Id.*

139. Robert R. Harrison, *Obtaining Medical Records After HIPAA: New Federal Privacy Protections Change the Rules for Attorneys*, 16 UTAH B.J. 16, 19 (2003).

140. Francis, *supra* note 110.

141. *Id.*

142. *See* Corley, *supra* note 15, at 504.

143. *Id.*

144. Adam J. Kolber, *Pain Detection and the Privacy of Subjective Experience*, 33 AM. J.L. & MED. 433, 454 (2007).

145. *Id.*

146. Francis, *supra* note 110 (internal quotation marks omitted).

147. *Id.*

elaborate on what constitutes as "more than necessary," consequently allowing anyone directly involved in the treatment of a patient to access a patient's general medical records.[148] This loophole allowed Galvin's insurance company to obtain more information about her than necessary while still complying with HIPAA.[149]

D. PROPOSAL TO STRENGTHEN PRIVACY PROTECTION FOR PSYCHOTHERAPY NOTES

Disclosures of psychotherapy notes embedded in general medical records harm individuals. Congress must provide a private right of action for citizens due to these potential financial and emotional harms. Additionally, lawmakers must strictly define the term "psychotherapy notes," and regulate the encompassed information to better protect patients.

1. Private Right of Action

The Clinton Administration and the HHS supported the notion of providing patients with a private right of action under HIPAA.[150] In the preliminary stages of HIPAA, former HHS Secretary Donna Shalala promoted private enforcement "[o]nly if we put the force of law behind our rhetoric can we expect people to have confidence that their health information is protected, and ensure that those holding health information will take their responsibility seriously."[151] Congress did not act on these recommendations, thus the HHS Secretary and the Office of Civil Rights (OCR) are solely responsible for enforcing HIPAA violations.[152] Congress's deliberate omission of private enforcement rights may be due to the fear of increasing litigation and overburdening the courts.[153] Although these are reasonable concerns, Congress should include a private right of action specifically for psychotherapy note related breaches because of the social stigma that is associated with mental health conditions.

Lawmakers should further create a private right of action against negligent disclosures by psychotherapists, similar to the private right of action Congress built into the Fair Credit Reporting Act (FCRA) against negligent disclosures by credit agencies.[154] Congress must recognize that a social stigma for mental illness persists, and that many individuals are afraid to seek treatment fearing that if discovered they could be subject to alienation by family and friends,

148. Corley, *supra* note 15, at 494.

149. Kolber, *supra* note 144, at 454.

150. Joshua D.W. Collins, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, 222–23 (2007).

151. *Id.* at 203.

152. *See* 65 Fed. Reg. 82462-01 (Dec. 28, 2000).

153. Collins, *supra* note 150, at 224.

154. Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1114-2 (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C. (2012)).

public humiliation, or losing their job.[155]

The Fourth Circuit Court of Appeals case, *Sloane v. Equifax Info. Servs., LLC*,[156] sheds light on the humiliation and emotional distress that privacy breaches create. Plaintiff, Suzanne Sloane, entered the hospital to deliver a baby.[157] While at the hospital, an employee noticed similarity in the womens' names and birthdates.[158] The employee stole Sloane's identity and began using her social security number to obtain credit cards, cash advances, and other goods totaling more than $30,000.[159] The identify theft affected Sloane's credit, which prevented her from buying a car and a home, caused her serious health problems, and led to the deterioration of her marriage.[160] Sloane filed a private right of action against the credit card agency under the FCRA and was awarded damages for the emotional distress, mental anguish, and humiliation she endured.[161]

Victims of a breach of psychotherapy notes need the same type of private recourse that the FCRA provides, because the release of sensitive information about a person's mental health can have a similar impact, if not worse, to that in *Sloane*.[162]

2. Broaden the Definition of Psychotherapy Notes

The Privacy Rule must be broadened to reflect HIPAA's initial goal of maintaining higher standards for the protection of psychotherapy notes.[163] Lawmakers should redefine psychotherapy notes to include more information generally amassed in psychotherapy sessions and treatments. Currently, the definition of psychotherapy notes excludes information about prescriptions, clinical test results, patient diagnoses, treatment plans, symptoms, progress to date, prognoses, and frequency of treatment.[164] This information contains sensitive data that demands greater protection.

Redefining psychotherapy notes to include more information about patient treatment, and creating best practice guidelines for psychotherapists regarding how the information is documented and stored will better protect patient privacy. More importantly, Congress should repeal the current rule giving psychotherapists the choice to either record information in psychotherapy notes or as part of the

155. Corley, *supra* note 15, at 503–04 (describing how HHS included anecdotes in the Privacy Rule of negative affects flowing from disclosure of mental illness data).

156. 510 F.3d 495 (4th Cir. 2007).

157. *Id.* at 498.

158. *Id.*

159. *Id.*

160. *Id.* at 498–99.

161. *Id.* at 507.

162. *See* Corley, *supra* note 15, at 504; *Sloane*, 510 F.3d at 495.

163. Leslie P. Francis, *New Perspectives on Guardianship and Mental Illness: Skeletons in the Family Medical Closet: Access of Personal Representatives to Interoperable Medical Records*, 4 ST. LOUIS U. J. HEALTH L. & POL'Y 371, 376 (2011).

164. *Id.*

general medical record, and implement strict provisions regarding the types of information that must be recorded as psychotherapy notes.[165]

CONCLUSION

Current law governing the protection of health information is problematic because it is antiquated and does not address modern concerns protecting health information, and it is comprised of broad language that creates loopholes, allowing covered entities and business associates to commit evasive practices.

It has been over a decade since HIPAA's enactment.[166] Subsequently, there has been a steady increase in "commercial collection, compilation, and exploitation of personal data" with the rise of Internet platforms such as social networking sites, and private Internet companies like WebMD and Netflix.[167] The proliferation of personal data available in cyberspace allows de-identified data to be linked to a specific person, and thus requires lawmakers to pass new laws.[168]

Congress must amend HIPAA to better protect medical health information. Congress should look to the underlying principles behind HIPAA's enactment and incorporate solutions to contemporary issues to strengthen privacy protection. The new provisions should require patient consent to disclose data, and provide them with the ability to track the whereabouts of their information. This would give patients a chance to stop the flow of information whenever the patient feels their information is being compromised in a way they deem unfit. A private right of action would then provide harmed patients with a proper form of redress. In addition, Congress should strengthen the definition of psychotherapy notes, by giving doctors less discretion and providing them better guidance to avoid over-inclusiveness or under-inclusiveness of information contained in general medical records. These proposals provide greater protection for medical information in an age of incessant sharing of personal information, while allowing the flow of information to researchers and medical personnel who use the information to better medical science and treatments.

---

165. Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers*, 1 DREXEL L. REV. 216, 250 (2009).

166. Collins, *supra* note 150, at 201.

167. Gellman, *supra* note 46, at 36.

168. *Id.*