MITCHELL | HAMLINE School of Law

Mitchell Hamline Law Review

Volume 45 | Issue 1 Article 11

2019

# Identities in Critical Condition: The Urgent Need to Reevaluate the Investigation and Resolution of Claims of Medical Identity Theft

Stephanie Lindgren

# IDENTITIES IN CRITICAL CONDITION: THE URGENT NEED TO REEVALUATE THE INVESTIGATION AND RESOLUTION OF CLAIMS OF MEDICAL IDENTITY THEFT

Stephanie Lindgren†



## I. INTRODUCTION

Imagine that you are planning the purchase of your first home. Like many first-time home owners, you apply for a loan from the bank. Your excitement flourishes when the bank calls you because you believe that the bank has approved your loan and that you are one

† JD Candidate, Mitchell Hamline School of Law, 2019; BS Political Science, University of Wisconsin–River Falls, 2015. I would like to thank Professor Thaddeus Pope for his guidance throughout the writing of this article. I would also like to thank the staff of Mitchell Hamline Law Review for their hard work. And finally, I wish to thank my amazing family—especially my fiancé, Ben—for all their love and support throughout law school.

step closer to owning your own home. However, the news you receive is not so exciting. The bank tells you that your loan was denied because of an outstanding medical bill on your record. You become confused and shocked because you have not received any medical treatment and are not aware of any outstanding bills.

Craig Murdock and his wife found themselves in this exact situation in 2015.[1] While trying to secure a loan for the Murdocks' first home, Craig discovered a medical bill for a heart procedure that he never underwent. Craig spent months trying to convince the hospital that he was a victim of identity theft before Craig eventually settled and paid the bill.[2] Unfortunately, medical identity theft is becoming increasingly common.[3]

The process of resolving medical identity theft places an extreme burden on victims to prove that they are not the individual who received treatment under their name.[4] However, meeting this burden can be impossible in some cases, causing the victims to bear the financial loss of paying for hospital services that they never received.[5] This article examines potential methods to revamp the current system and shift the burden of researching and resolving cases of medical identity theft to healthcare providers.

This article begins with a general overview of the history of identity theft in general and then specifically discusses the current state of medical identity theft.[6] This article further examines how and why medical identity theft occurs.[7] Next, it discusses the personal impact that medical identity theft has on victims and how victims can respond to medical identity theft and altered medical records.[8] Next, the article covers the current laws and regulations governing medical identity theft and the evolution of these laws and regulations over

1. Courtney Gerrish, *Woman Steals Identity to Procure Liver Transplant*, WTMJ-TV MILWAUKEE (Nov. 3, 2015), http://www.tmj4.com/news/i-team/medical-identity-theft [https://perma.cc/EY5L-7TPE] (showcasing the effects that a stolen medical identity can have on a victim).

2. *Id.*

3. *Id.*

4. *See* Joseph Menn, *ID Theft Infects Medical Records*, L.A. TIMES (Sept. 25, 2006), http://www.pnhp.org/news/2006/october/id-theft-infects-medical-records [https://perma.cc/K9LX-UPML].

5. *Id.*

6. *See infra* Parts II.A., B.

7. *See infra* Part II.B.

8. *See infra* Part II.C.

time.[9] The article then turns to available legal remedies and the harm that medical identity theft victims suffer.[10] It then analyzes several recommendations regarding how to respond and improve the ease with which victims can resolve claims.[11] Finally, this article recommends that healthcare providers should bear the responsibility for researching cases of medical identity theft that have occurred within their institutions.[12]

## II. IDENTIFYING IDENTITY THEFT

### *A. Identity Theft Generally*

Identity theft is a fast-growing problem, with seven percent of individuals over the age of sixteen falling victim to identity theft in 2014.[13] Fifteen percent of persons age sixteen or older—36.5 million people—will experience some form of identity theft at some point in their life.[14] Identity theft occurs when "a thief steals your personal information, such as your full name or social security number, to commit fraud."[15] Although financial identity theft is often the first thing to come to mind when people hear the term "identity theft," more than 250,000 cases of medical identity theft were reported between 2001 and 2006.[16] Medical identity theft is the theft of personal information for the specific purpose of obtaining healthcare-related services, such as prescriptions, personal medical treatments, and surgeries.[17] Although medical identity theft and financial identity theft are similar, medical identity theft is far more personal because medical identity theft has the possibility of negatively affecting an

9. *See infra* Parts III.A.–E.

10. *See infra* Part III.F.

11. *See infra* Part IV.

12. *See infra* Part V.

13. ERIKA HARRELL, VICTIMS OF IDENTITY THEFT, 2014 1 (2017) https://www.bjs.gov/content/pub/pdf/vit14.pdf [https://perma.cc/5TBS-3URR] (providing general statistics on cases of identity theft).

14. *Id.* at 13.

15. *Identity Theft*, USA.GOV, https://www.usa.gov/identity-theft [https://perma.cc/QC2U-YVN2].

16. Whitney Walters & Axton E. Betz, *Medical Identity Theft*, 29 J. CONSUMER EDUC. 75, 75 (2012) (explaining the differences between financial identity theft and medical identity theft and the prevalence of each).

17. *Id.*

individual's future medical treatment, such as receiving an incorrect diagnosis or prescription.[18]

There is no debate that financial identity theft is a major problem in our current society and that victims of this crime suffer enormously. However, victims of financial identity theft can protect themselves by demanding that credit bureaus correct their record based on the Fair Credit Reporting Act.[19] Unfortunately, victims of medical identity theft do not have similar recourses available to them.[20]

Data breaches are an enormous threat and concern to citizens and lawmakers in the United States because of the massive amount of private information that thieves can steal in one instance.[21] Federal legislation distinguishes between financial identity theft and medical identity theft.[22] This legislative distinction is based on the public's heightened expectation of privacy regarding personal medical information.[23] The rest of this section will examine how thieves commit medical identity theft and the current problems facing the healthcare industry because of the continued growth of medical identity theft.

Institutions storing individuals' personal information have a duty to ensure that the information is protected.[24] The difficulty in

18. PAM DIXON, MEDICAL IDENTITY THEFT: THE INFORMATION CRIME THAT CAN KILL YOU 6 (2006), http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf [https://perma.cc/M65X-LB7T].

19. *Id.* at 3.

20. *Id.* at 40.

21. Stanley C. Ball, Note, *Ohio's "Aggressive" Attack on Medical Identity Theft*, 24 J. L. & HEALTH 111, 122 (2010) (suggesting the development of a national system using Ohio's Data Breach Notification Statute as a framework to combat medical identity theft). The national system would only apply to medical identity theft that occurs as a result of data breaches in healthcare provider institutions. *Id.* at 133–38. Other forms of medical identity theft would not be covered under this system. *Id.*

22. *Id.* at 122.

23. *See id.* The public has given medical information heightened scrutiny because of the ability of medical information to affect future medical treatment and diagnosis and because of the extreme difficulty in proving and resolving claims. *Id.* Most individuals would consider medical information extremely personal and essential to protect. *Id.*

24. *The HIPPA Privacy Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [https://perma.cc/5S2C-ENPZ] ("The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care

properly storing this data occurs when identity thieves undermine the system of data collection and storage. One hacker has the potential to cripple an entire company, leaving unexpected and substantial destruction in their wake.[25] Regulations should require healthcare providers to inform patients when their systems are breached and personal information is exposed.[26] However, because these entities have an interest in keeping data breaches secret, potential victims of medical identity theft are often left without notice of a data breach.[27]

### *B. Medical Identity Theft: What, How, and Why?*

Medical identity theft, which occurs "when someone steals your personal identification number to obtain medical care, buy medication, or submit fake claims to your insurer or Medicare in your name," is a particularly personal form of fraud.[28] Medical identity theft is uniquely attractive to thieves because of the many ways that thieves can use stolen medical information.[29]

One of the most notorious examples of medical identity theft occurred in 2006 when Lind Weaver received a bill for the amputation of her right foot despite still having both of her feet.[30] Weaver spent more than a year trying to clear her medical record of the error, but was unsuccessful.[31] While continuing her effort to clear up the issue, Weaver suffered a heart attack and was taken to the hospital.[32] Several days later, Weaver awoke to a nurse asking her what medications she takes to treat her diabetes.[33] Weaver informed the nurse that she had never been diagnosed with diabetes or treated for

clearinghouses, and those health care providers that conduct certain health care transactions electronically.").

25. Ball, *supra* note 21, at 115.

26. *Id.* at 140.

27. *Id.* at 139–40 (explaining that an organization may choose to disclose data breaches under certain current regulations).

28. *Identity Theft*, *supra* note 15.

29. Walters & Betz, *supra* note 16, at 75 (stating that stealing an individual's personal medical information is attractive to a thief because the thief can obtain prescriptions, receive routine medical treatments, or even have surgery using the stolen medical identity).

30. *See* Menn, *supra* note 4 (illustrating an egregious example of what is required for an individual to prove that they were not the individual who received the treatment for which they are now being billed).

31. *Id.*

32. *Id.*

33. *Id.*

the disease.[34] As it turned out, the thief that stole Weaver's identity not only received a foot amputation but also had diabetes. Both the amputation and diagnosis of diabetes were entered into Weaver's chart.[35] If Weaver had not woken up, the nurse might have given Weaver insulin—potentially killing her.[36] This case illustrates the unique harm that medical identity theft creates: the harm is not just financial—it can affect patient treatment and could cost someone their life.

Another example of the distinct danger posed by medical identity theft occurred when Anndorie Sachs, a mother of four, received a $10,000 hospital bill and notification that her newly born baby tested positive for illegal drugs.[37] Although Sachs had not given birth recently, the hospital would not accept that Sachs was not the patient and insisted she was the mother of the child.[38] The situation became extreme when police officers showed up at Sachs's door intending to take her four children and place them in protective services based on the results of the drug test.[39] All of this arose because a thief stole Sachs's driver's license and gave birth under Sachs's name to a child who tested positive for drugs.[40] Once the hospital placed this erroneous information on Sachs's medical record, it was extremely

34. *Id.*

35. *Id.* (stating that diabetes is a disease that can lead to foot problems that could require amputation).

36. *Id.* Here, the hospital called a collection agency and Weaver's credit score was ruined. *Id.* It wasn't until Weaver threatened the hospital with litigation that the hospital agreed to drop Weaver's bill; however, the insurance company refused to pay the hospital bill because Weaver was not the patient who received treatment. *Id.*; *see* Lorelei Laird, *Federal Medical-Privacy Law Frustrates ID Theft Victims*, ABA J. (Sept. 2014), http://www.abajournal.com/magazine/article/federal_medical-privacy_law_frustrates_id_theft_victims [https://perma.cc/Z7HR-9554] (explaining the frustration that many victims of medical identity theft must endure when attempting to prove and resolve claims of medical identity theft).

37. *See* Caitlin A. Johnson, *Protect Against Medical ID Theft*, CBS NEWS (Oct. 9, 2006), http://www.cbsnews.com/stories/2006/10/09/earlyshow/living/ConsumerWatch/main2073225.shtml [https://perma.cc/W9M7-P24E] (showcasing the devastating effect that medical identity theft can have on a victim and their family). Some hospitals, such as the University of Connecticut Health Center, have started asking patients for proof of identification before inputting any information into patient records. *Id.*

38. *Id.*

39. *Id.*

40. *Id.*

difficult for Sachs to correct it.[41] As of October 2006, Sachs was still unsure if the thief's medical information remained entangled with her own.[42] Individuals such as Weaver and Sachs are forced to go through life with the constant fear that incorrect information in their medical records could disturb their livelihood, result in harmful treatments, or even cause their death.

Most medical identity theft cases never make it to court because of the difficulty in identifying the individual who caused the harm.[43] However, in 1996 a case went to trial when a psychiatrist altered patient records to fraudulently bill for services that the psychiatrist never rendered; sometimes for individuals who were not even patients.[44] Additionally, the psychiatrist falsely reported severe diagnoses such as depression, abuse, or drug addiction.[45] The court described the harm that the psychiatrist bestowed upon these patients and non-patients:

> Whether it should or not, the misinformation will almost certainly have an impact on patients' lives. It may determine whether an individual will be given a health insurance policy; it may decide whether he or she will receive government clearance; it may affect a whole host of other situations. Dr. Skodnek's abuse of trust—and its unquestionable impact on his patients' lives and the lives of their family members—are very, very troubling. And, what is unusual about this fraud scheme is not that Dr. Skodnek "puffed" the time he spent but went much, much further. He

41. *Id.* (stating that Sachs "had to take a DNA test to prove she wasn't the mother of the drug-addicted baby").

42. *Id.*

43. KAMALA D. HARRIS, MEDICAL IDENTITY THEFT: RECOMMENDATIONS FOR THE AGE OF ELECTRONIC MEDICAL RECORDS, 1 (2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf [https://perma.cc/QU22-EKZU] ("Medical identity theft is often underreported, as it is difficult to detect . . . ."); James Swann,*Warning: Your Medical Identity May Not Be Safe*, BLOOMBERG NEWS (May 22, 2018), https://www.bna.com/warning-medical-identity-n57982092785 [https://perma.cc/J3HQ-AH4L] ("There's no way to trace a specific case of medical ID theft back to a specific data breach, but providers are under pressure to secure patient data and prevent it from getting into the wrong hands.").

44. United States v. Skodnek, 933 F. Supp. 1108, 1114 (D. Mass. 1996) (explaining the various ways that a victim will be harmed by having their identity stolen and their medical records falsely altered without their knowledge). This was one of the few cases of medical identity theft that actually made it to trial and in which the court found that an individual perpetrator was responsible. *Id.* at 1123.

45. *Id.* at 1121.

> created a paper trail for these patients out of whole cloth, inventing histories of mental health treatment with which those individuals must now contend.[46]

These are only a few examples of ways that medical identity theft can affect a victim's life. Although they are extreme examples, these situations could happen to anyone; thieves can steal medical identities and use them to bill the victims' insurance plans for services that the victims never received. Healthcare provider employees who are attempting to turn a quick profit most commonly perpetrate this form of identity theft, which rises to the level of medical identity fraud.[47] The employee can steal the medically identifiable information and sell it to a third party who is "seeking to commit the fraud."[48] More often than not, medical identity theft is an "insider" crime.[49]

There are a variety of ways that thieves can steal a person's personal information. The most popular method is through acquiring the victim's social security number.[50] A social security number is not as hard to obtain as one might think. Healthcare and financial industries compile personal information—including social security numbers—and share the information with each other, providing various opportunities for a third-party to hack or steal the information.[51] One author, Stanley Ball, explained the four most common reasons that medical identity theft is perpetrated:

46. *Id.*; *see also* DIXON, *supra* note 18, at 5–6 (describing the many ways that medical identity theft harms victims, including the alteration of the victim's medical records).

47. Katherine M. Sullivan, Note and Comment, *But Doctor, I Still Have Both Feet! Remedial Problems Faced by Victims of Medical Identity Theft*, 35 AM. J.L. & MED. 647, 650–51 (2009) (explaining the different ways that an individual could gain access to and steal a victim's identity). A lone individual who is desperate for health services may perpetrate this crime or a ring of individuals may steal medical identities to extort money from insurance companies. *Id.*

48. *Id.* at 651.

49. DIXON, *supra* note 18, at 36. Generally, cases of medical identity theft will involve some kind of healthcare professional; either at the provider or insurance level. *Id.* Individuals inside healthcare organizations have easier access to medical records. *Id.*

50. R. Bradley McMahon, Note, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why is Identity Theft the Most Prevalent Crime in America?*, 49 VILL. L. REV. 625, 627 (2004) (describing the importance of an individual's social security number in securing personal information and in its use as an identifier, especially when a photo ID is not required).

51. *Id.* at 628–29 ("The liberal sharing policies of companies allow personal information to flow far beyond primary compilers.").

> (1) "A person uses . . . the identity of another . . . to obtain medical care because the [person] is uninsured." (2) "A [person] uses the identity of another to obtain medical care because the [person] does not want [his] health records to include information about his . . . health status." Specifically, the identity thief desires to prevent his current or future employer, or "insurance provider from knowing aspects of [his] true health condition." (3) A person uses the victim's identity to obtain a drug prescription for recreational use or criminal distribution. (4) A person obtains the victim's health information. Then in a separate incident, the thief also steals the personal identifying information needed to pose as a physician and submits claims for reimbursement to an insurance provider for services never rendered to any individual. This is not uncommon and can "involve hundreds of identities and the submission of millions of dollars' worth of false claims.[52]

It is important to first understand how a thief is able to gain access to a patient's personal information. When a patient goes to a medical provider, the provider generally asks the patient to provide registration information for hospital records.[53] This information may include the patient's name, date of birth, address, insurance information, racial background, and social security number.[54] The provider places this information in the hospital's records for that specific patient. Next, the patient receives care from a physician during an office visit. The physician's office adds information discussed during the visit to the patient's medical records, including the patient's symptoms, diagnosis, and prescriptions.[55] Then, at the end of a visit, a physician inputs all care the physician rendered into

52. Ball, *supra* note 21, at 118 (numbering added) (quoting BOOZ ALLEN HAMILTON, MED. IDENTITY THEFT ENVTL. SCAN 4–6 (2008), https://www.healthit.gov/sites/default/files/hhs_onc_medid_theft_envscan_101008_final_cover_note_0.pdf [https://perma.cc/7VQN-AZFV]).

53. *See generally* Thomas Clifford, *Provider Liability and Medical Identity Theft: Can I Get Your (Insurance) Number?*, 12 NW. J.L & SOC. POL'Y 45, 50 (2016) (explaining the process of patient information gathering in hospitals and how that information is transferred and stored). Because patient information passes through so many different hands and agencies, there are many points at which a thief could steal the information without raising alarms. *Id.*

54. *Id.*

55. *Id.*

the patient's record and sends charges to the insurance company for approval.[56]

Once the insurance company reviews the services that the physician provided, the insurance company sends the patient an Explanation of Benefits statement that discloses the amount the insurance company will pay.[57] The hospital then sends the patient a bill for the remaining balance.[58] Because all these different hands touch patient medical records, it is difficult to ensure that records are protected.

To understand how easy it is to find and steal an individual's health information and identity, consider this example. In the 1990's, the Group Insurance Commission (GIC) released records to the public that included a summary of hospital visits by state employees in Massachusetts.[59] The GIC gave the files to researchers at no cost.[60] The GIC removed identifying information such as names, addresses, and social security numbers before releasing the files.[61] The GIC believed the files to be "de-identified" and safe to release for research.[62] However, information such as birth date, sex, and zip code remained on the files.[63] A student then purchased the voter rolls for Cambridge, Massachusetts, and set about finding the governor of Massachusetts's personal health history.[64] Using this "de-identified" information, the student was able to determine that only "[s]ix people in Cambridge shared the Governor's birth date, only three were men, and the governor was the only one in his zip code."[65] This case demonstrates just how easy it is for medical identity thieves to connect various forms of public information to find medical information about an individual.

Data breaches are the most prevalent form of medical identity theft.[66] Data breaches occur when there is an "unauthorized

56. *Id.*
57. *Id.* at 51.
58. *Id.*
59. *Id.* at 49.
60. *Id.*
61. *Id.* at 49–50.
62. *Id.* at 49.
63. *Id.* at 50.
64. *Id.* ("Voter rolls included the name, address, zip code, birth date, and sex for each voter.").
65. *Id.*
66. Paige Schaffer, *Healthcare Data Breaches Open a Pandora's Box of Patient Identity Theft*, DIGITAL COMMERCE 360 (Sept. 8, 2017), https://www.digitalcommerce3

acquisition, access, use or disclosure of protected health information."[67] This article further discusses data breaches in Part V.

### *C. Harm Suffered by Victims*

Medical identity theft affects many parties, including the healthcare provider, the insurance company, and the victim.[68] The primary victim is the individual whose medical information and identity has been stolen.[69] The victim can experience a lasting impact that may far outweigh and outreach the consequences of financial identity theft.[70] For example, if the thief used the victim's medical information to obtain health services, such as treatment or surgery, those records remain on the victim's health history—sometimes without the victim ever knowing that the history is incorrect.[71] Medical identity theft can also negatively impact the victim's ability to obtain insurance coverage. If the victim needs medical care or service, but the thief already received that service by using the victim's identity, the insurance provider may deny covering the cost.[72]

A victim may experience many other lasting effects of medical identity theft; the least of which is simply the time, energy, and finances that it takes for the victim to correct the issue and to prove that their identity was stolen.[73] Individual victims may spend as many as thirty hours researching, resolving, and recovering from the misuse of their medical information.[74] It may take even more time for victims to amend medical records that contain false information.[75]

60.com/2017/09/08/healthcare-data-breaches-open-a-pandoras-box-of-patient-identity-theft [https://perma.cc/H8KB-9T3K]; *see also* Joseph D. Szerejko, Note, *Reading Between the Lines of Electronic Health Records: The Health Information Technology for Economic and Clinical Health Act and Its Implications for Health Care Fraud and Information Security*, 47 CONN. L. REV. 1103, 1122, 1127 (2015) (examining the effect that the shift to electronic storage of information will have on patients and healthcare providers in cases of medical identity theft).

67. Szerejko, *supra* note 66, at 1122.

68. Sullivan, *supra* note 47, at 651 (examining all the ways in which medical identity theft affects victims in the short-and long-term).

69. *Id.*

70. *Id.*

71. *Id.* at 651–52 (explaining how medical providers rely on a patient's medical history as a complete and accurate account in diagnosing and treating a patient).

72. *Id.* at 652.

73. *Id.*

74. *See* Dixon, *supra* note 18, at 30.

75. *Id.*

Nikki Burton was seventeen years old when she wanted to donate blood for the first time.[76] However, when Burton went to donate the donation center turned her away without any explanation.[77] Burton was confused about this rejection and contacted the Red Cross for information.[78] The Red Cross informed Burton that Burton's file listed her as barred from donating blood because Burton's social security number had been used to obtain AIDS treatment.[79] Burton was very confused, as she did not have AIDS.[80] Burton discovered that a thief had stolen her social security number and that an imposter had used her identity to receive treatment.[81]

In a separate case, the medical records of a woman who was about to have bypass surgery listed her height as just over five feet.[82] In reality, this woman was over six feet tall; if the medical staff had not caught the error in time, the woman could have suffered serious complications during surgery.[83]

Healthcare providers and insurance companies are the secondary victims of medical identity theft, given that primary victims generally refuse to pay for services or medication they did not receive.[84] Incidents of medical identity theft could also result in negative publicity for the business because data breaches decrease customer confidence.[85]

Additionally, healthcare providers that rely on inaccurate medical records for victims of identity theft could be subject to litigation.[86] Stanley Ball notes that the "cost of investigating crimes, prosecuting criminals, enforcing federal rules, and payouts to criminals as a direct fraud victim" affects federal agencies.[87] Society

76. Clifford, *supra* note 53, at 46 (listing several stories of victims of medical identity theft).

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id.*

82. *Id.*

83. *Id.* (stating that a dosage based on a height more than one foot different from the patient's actual height could have devastating consequences because anesthesia dosage is calculated based on height and weight).

84. *See* Sullivan, *supra* note 47, at 652–53 (stating that the provider will not make the victim pay for the thief's bill if the victim can prove they were not the individual who received treatment).

85. *Id.*

86. *See id.* at 666.

87. Ball, *supra* note 21, at 121.

also suffers because offsetting the costs of fraudulently received services requires patients to pay more for legitimate services.[88] Victims may suffer the most lasting impact from a lowered credit score due to outstanding medical bills for the thief's medical care.[89] Victims could also have inaccurate medical history records, potentially leading to incorrect diagnoses and treatments.[90]

## III. REGULATIONS AND LEGAL REMEDIES FOR VICTIMS

Once an individual's medical identity is stolen, no set framework exists for victims to correct the error.[91] The "current remedies available to victims leave something to be desired" because the "burden is entirely on the victim to navigate the healthcare system, track down all of the disparate record custodians, and convince the custodians of the victim's right to amend their records."[92] The Office of the Inspector General provides information for various agencies that victims may contact when their identity is stolen.[93] However, the guidance from these agencies is often tangled and unclear, including multiple referrals to different agencies and no clear answers on how to address medical identity theft.[94]

The Federal Trade Commission (FTC)'s website contains a link to a brochure that walks healthcare providers through the process of researching claims and counseling patients on how to respond to medical identity theft.[95] This brochure seems helpful at first, laying

88. *Id.*

89. Sullivan, *supra* note 47, at 652.

90. *See* Walters & Betz, *supra* note 16, at 76–77 (explaining the impact of incorrect medical records on a patient's future medical treatment).

91. *See Medical Identity Theft*, FED. TRADE COMMISSION (Sept. 2018), https://www.consumer.ftc.gov/articles/0171-medical-identity-theft [https://perma.cc/T3FG-K8SZ] [hereinafter FTC] (providing a checklist for "How to Correct Errors in Your Medical Records"); *see also* FED. TRADE COMM'N, IDENTITY THEFT: A RECOVERY PLAN 15 (Sept. 2018) (providing a checklist for "Medical Identity Theft").

92. Sullivan, *supra* note 47, at 674 (explaining that there is currently no help available to victims in researching and attempting to prove or resolve their claims of medical identity theft).

93. *Contact Us*, OFF. INSPECTOR GEN., https://oig.hhs.gov/contact-us/index.asp [https://perma.cc/6KD6-MWXF] (providing contacts to "[r]eport misuse of your personal information, including your Medical Identity," "[r]eport suspected Medicare fraud related to Medical Identity Theft," "[r]eport questionable charges to Medicare," and adding that "[y]ou can also contact your local Senior Medicare Patrol").

94. *See id.*

95. FTC, *supra* note 91.

out a basic "to-do" list for providers.[96] However, the brochure is not at all helpful to a victim who is dealing with a healthcare provider who does not follow the FTC's protocol.[97] Usually, a victim must fight for years before a provider accepts that the victim is not the individual responsible for the fraudulent bill and that the provider should not force the victim to pay the bill.[98] The brochure minimizes how difficult and extensive the process is for victims.[99] Victims must contact every potential healthcare provider with whom a thief could have used the victim's identification to determine whether the provider entered incorrect information into the victim's medical history file.[100] The brochure also does not explain how to respond to providers who refuse to supply victims with their medical records for fear of violating HIPAA rights.[101] Victims need a more extensive framework for walking through a standard process for resolving their claims.[102] Current resources do not provide victims with straight answers on how to resolve their claims.

Congress attempted to abate this problem through four different laws[103]: (1) the Identity Theft and Assumption Deterrence Act (ITADA) in 1998;[104] (2) the Health Insurance Portability and Accountability Act (HIPAA) in 1996;[105] (3) the Gramm-Leach-Bliley Act (GLBA) in 2001;[106] and (4) the Health Information Technology for Economic and Clinical Health Act (HITECH) amendment to HIPAA in 2009.[107]

96. *Id.*

97. *See generally* Sullivan, *supra* note 47, at 660–64 (discussing the challenges victims face when trying to report and resolve their stolen medical identities).

98. *Cf.* Szerejko, *supra* note 66, at 1152 ("Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years.").

99. *Id.*

100. *Id.*

101. FTC, *supra* note 91 (explaining how the provider should respond to a victim's request for their own medical records under HIPAA).

102. Sullivan, *supra* note 47, at 678.

103. Ball, *supra* note 21, at 126–27; McMahon, *supra* note 50, at 629.

104. McMahon, *supra* note 50, at 629.

105. *Id.*

106. *Id.*

107. Ball, *supra* note 21, at 126.

### *A. ITADA*

The ITADA was the first federal law to provide punishment for stealing an individual's personal information or for possessing stolen identification with the intent to defraud the United States government.[108] The ITADA provides punishment for all forms of identity theft; not only medical. Punishments range from fines to prison time up to fifteen years.[109] The ITADA is not limited to punishing only fraudulent uses of an individual's social security card; courts even consider the "misuse of a person's name alone, without other identifying information" to be an unauthorized use of the identification of another person and in violation of the ITADA.[110] Congress intended the act to serve as a deterrent to any would-be identity thief; however, the act has not been effective.[111]

The ITADA has been ineffective because of its focus on punishment and after-the-fact fixes. For example, the ITADA does not provide a solution for preventing identity theft or how to apprehend thieves once they have stolen someone's identity.[112] Since the ITADA contains little material that details how to apprehend a thief, "the risk of suffering a penalty is well worth the reward for a potential thief."[113]

### *B. HIPAA*

The second law, HIPAA, most effectively deters and limits cases of medial identity theft.[114] HIPAA's purpose is to provide a framework for the transfer and sharing of private information between

108. 18 U.S.C. § 1028(a) (2003). *See generally* United States v. Wong, No. 14-10294, 2015 U.S. App. LEXIS 12747 (9th Cir. July 23, 2005) (finding a violation of the Identity Theft Act).

109. 18 U.S.C. § 1028(b).

110. Wong, 2015 U.S. App. LEXIS 12747 at *5 ("A 'means of identification' is 'any *name* or number that may be used, *alone* or in conjunction with any other information, to identify a specific individual.'" (quoting 18 U.S.C. § 1028(d)(7)) (emphasis added)).

111. McMahon, *supra* note 50, at 630–33. S*ee generally* 18 U.S.C. § 1028.

112. McMahon, *supra* note 50, at 632–33; s*ee* 18 U.S.C. § 1028.

113. McMahon, *supra* note 50, at 633 (explaining the ease with which thieves can steal an identity and why the benefits of doing so outweigh any risks for thieves).

114. *See generally id.* at 644–45 (describing the purpose and enactment of HIPAA).

healthcare institutions.[115] Moreover, HIPAA attempts to make it easier for employees to retain the same health insurance when transferring jobs.[116] Even though Congress enacted HIPPA in 1996, the act did not go into effect until April 2003.[117] HIPAA covers privacy policy in health plans, healthcare clearinghouses, and healthcare providers who electronically transmit any health information in connection with transactions for which Health and Human Services has adopted standards.[118] The specific sections of HIPAA that relate to health information privacy are the "Privacy Rule" and the "Security Rule."[119] HIPPA limits the situations in which a covered entity can disclose a consumer's personal information to a third party.[120] HIPPA's limits require a patient's explicit written consent before a covered entity can disclose the patient's personal information to a third party.[121]

Specifically, the Privacy Rule focuses on regulating disclosure of health information.[122] The Privacy Rule also allows individuals to review and possibly amend their own medical records for accuracy.[123] The review and amendment portion of the rule is not absolute and the covered entity can deny any request from a patient.[124] HIPPA's lack of a requirement for providers to amend erroneous health information that a patient discovers is a large downfall, given that the provider will continue to use erroneous information when diagnosing and treating the patient.[125]

115. *Id.* at 644 ("[M]ore than seventeen organizations may handle a single medical record, and approximately four hundred people may see a patient's medical record during one hospital stay.").

116. Sullivan, *supra* note 47, at 657.

117. McMahon, *supra* note 50, at 645; Sullivan, *supra* note 47, at 658 (explaining that the Secretary of Health and Human Services (HHS) added the Security Rule in 2003 under the simplification section of HIPAA, and that HHS oversees the security and privacy requirements of the Security Rule).

118. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

119. Sullivan, *supra* note 47, at 659.

120. *See* § 1177(a)(3), 110 Stat. at 2029.

121. McMahon, *supra* note 50, at 648. This is called the "Opt-In Provision" of HIPAA. *Id.*

122. Sullivan, *supra* note 47, at 659–60.

123. *Id.*

124. *Id.* at 660 (stating that providers are not required to allow patients to review or amend any medical information that the approving provider did not create).

125. *Id.* at 661.

HIPAA also contains language allowing individuals to seek an amendment to their medical records.[126] However, HIPPA only requires a provider to make an amendment to medical information that the provider or insurer created and maintains.[127]

The main criticism of HIPAA is that there are too many exceptions that undermine the law's purpose.[128] Another criticism is that there is not a proper enforcement mechanism through HIPAA.[129] Victims do not have a private cause of action to receive reimbursement for what they have lost. Only administrative agencies, not individuals, can enforce HIPAA and impose either the monetary penalties or prison sentences.[130]

### *C. GLBA*

The third law Congress enacted to address identity theft was the Gramm-Leach-Bliley Act (GLBA).[131] This law specifically protects personal information in financial services.[132] The GLBA focuses on holding financial institutions responsible for protecting the personal information of their customers.[133] The GLBA does three basic things: (1) requires a financial institution in specified circumstances to provide notice to customers about its privacy policies and practices; (2) describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to

126. DIXON, *supra* note 18, at 40–41.

127. *Id.* HIPPA requires only the originating provider to correct errors in information that the originating provider sends to another provider or insurance company; it does not require receiving insurers or providers to make corrections. *Id.* Even if a physician corrects a patient's file, there is no guarantee that all the circulating records will also be corrected. *Id.* at 41. To further complicate the issue, many individuals will not be allowed to see their record in the first place because many providers are concerned that they will be in violation of HIPPA's privacy requirements if they allow an individual to view records listing services that the individual claims to have not received. *Id.*

128. McMahon, *supra* note 50, at 649 (explaining the downfalls of HIPAA and how HIPPA has lost its effectiveness in preventing medical identity theft in our current society).

129. *Id.*

130. *Id.* HIPAA also does not penalize third parties for abusing any personal information that they may receive from an institution covered under the law. *Id.* at 650.

131. Financial Services Modernization Act of 1999, Pub. L. No. 106-103, 113 Stat. 1338 (1999).

132. § 501, 113 Stat. at 1437.

133. *Id.*

nonaffiliated third parties; and (3) provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure.[134]

The GLBA contains the requirements that a financial institution must meet before the institution can "hand out" an individual's personal information to a third party.[135] When it was enacted, the GLBA was the most protective law yet for consumer privacy.[136] However, the GLBA still fell short of making a real difference in the way financial institutions handle personal information. The law created loopholes for institutions because of its ambiguous language.[137] Thus, individuals have little control over where their personal information ends up.[138] Additionally, no private cause of action exists for victims, which leaves victims ultimately responsible for any fraudulent charges under their name.[139]

### *D. HITECH Act*

In 2009, Congress amended HIPAA through the Health Information Technology for Economic and Clinical Health (HITECH) Act.[140] Under the HITECH Act, healthcare providers covered by HIPAA must notify individuals if their health information suffers a breach.[141] This requirement applies only to unsecured personal health information.[142] Once a breach is discovered, healthcare providers are required to provide notice to victims within sixty days and the notice must include each of the following:

134. *Id.* (describing the purpose of the GLBA).

135. McMahon, *supra* note 50, at 633–34. Minnesota initiated a lawsuit against U.S. Bank due to concerns that the bank was selling customers' personal information to telemarketers. Evidence later demonstrated that that some of the telemarketers used the information fraudulently. *Id.* The lawsuit gained national attention and the public soon realized that many large banks had been involved in similar practices of selling personal information to third parties. *Id.* at 634.

136. *Id.*

137. *Id.* at 640.

138. *Id.*

139. *Id.* at 643 (explaining that "only the FTC has the right to enforce the GLBA privacy provisions").

140. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, § 13001, 123 Stat. 226 (2009) (amending HIPAA to require institutions to notify all individuals that could possibly be affected by any data breach at that institution).

141. *Id.* § 13402, 123 Stat. at 260.

142. *Id.*

> (1)A brief description of what happened, including the date of the breach and the date the breach was discovered. . .; (2) A description of the types of unsecured protected health information that [was] involved in the breach. . .; (3) The steps individuals should take to protect themselves from potential harm resulting from the breach[;] (4) A brief description of what the covered entity is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and (5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.[143]

The attorney general of each state has the authority to enforce each of the provisions.[144] The relief that the HITECH Act awards is limited to an injunction or statutory damages.[145] The HITECH Act also states that any monetary penalty that a court grants must be paid by the healthcare provider to the Office for Civil Rights to "further enforce HIPPA's requirements."[146] Through the HITECH Act, victims can only recover damages if the state they reside in has decided to allow data-breach victims to receive a portion of the damages the provider pays to the Office for Civil Rights.[147]

### *E. Red Flags Rule*

In 2008, the Federal Trade Commission issued the Red Flags Rule, which requires hospitals and institutions to implement written identity-theft prevention programs.[148] These regulations seemed to

143. Ball, *supra* note 21, at 127–28 (citing HITECH Act, Pub. L. No. 111-5, § 13402(f), 123 Stat. 262 (2009)).

144. *Id.*

145. *Id.* (stating that the Office for Civil Rights is within the Department of Health and Human Services).

146. *Id.*

147. *Id.* at 128–29.

148. Michelino Mancini, *Medical Identity Theft in the Emergency Department: Awareness is Crucial*, WESTERN J. EMERGENCY MED. 899, 899–901 (2014) ("The first is identifying relevant red flags within an institution's day-to-day operations, such as alerts from credit reporting companies, altered or other suspicious documents, mismatched personal identifying information (i.e., incorrect social security number with stated address), fraudulent credit account activity and notices from other sources (i.e., law enforcement). The second element is to detect these relevant red flags through verification and authentication methods. The next element is to prevent and mitigate identity theft. This would include notifying a supervisor or law enforcement in order to monitor and investigate current and existing accounts.

be a step in the right direction because they placed responsibility solely upon healthcare providers. However, Congress dimmed that hope by passing the Red Flag Program Clarification Act (RFPCA) of 2010, which granted many providers an exemption from the Red Flags Rule.[149] The RFPCA effectively redefined what it means to be a "creditor."[150] The RFPCA regulates only creditors and the revised "creditor" definition almost exclusively exempts healthcare providers.[151]

Although healthcare providers that fall outside of the RFPCA's definition of "creditor" are exempt from this legislative change, these providers "would still need to develop" policies or strategies on how to prevent or otherwise handle cases of identity theft.[152] The Red Flags Rule seemed like a positive move toward protecting victims of medical identity theft, but, with the addition of the RFPCA, the Red Flags Rule ended up being another regulation that, in practice, did not protect victims at all. Even if Congress had not passed the RFPCA, the Red Flags Rule did nothing to allow individuals access to amend their affected medical records.[153]

### *F. Emerging Legal Remedies*

A new legal remedy is emerging to address medical identity theft. This remedy has come about in response to the current inadequate system, which provides no cause of action for victims seeking reimbursement.[154] Imagine that an individual receives a bill for a

Finally, the organization should maintain the program and remain up to date as identity theft tactics change and new technology, such as biometric software for iris scans and facial-recognition, becomes more readily available.").

149. *Id.* at 900.

150. John S. Servidio & Amy R. Worley, *Know Your Red Flags For The Identity Theft Red Flag Rule*, LAW 360 (April 16, 2014), https://www.law360.com/articles/520990/know-your-red-flags-for-the-identity-theft-red-flag-rule [https://perma.cc/7JXG-D4BS].

151. Chris Dimick, *Red Flags Clarification Exempts Most, Not All Providers*, J. OF AHIMA, (Dec. 16, 2010), http://journal.ahima.org/2010/12/16/red-flag-clarification-exempts-most-not-all-providers [https://perma.cc/39E3-AFYL]. The original definition of "creditor" was an entity that "provided a service upfront and collected payment later in installments, such as a hospital providing treatment to a patient and then setting up a payment plan." *Id.*

152. *Id.*

153. Sullivan, *supra* note 47, at 666.

154. Kirk J. Nahra, *Lessons Learned from Recent Privacy Litigation*, PRIVACY ADVISOR (Oct. 1, 2007), https://iapp.org/news/a/lessons-learned-from-recent-privacy-

medical service that the patient did not receive, or a bill for medication not prescribed to them—it is a fair assumption that this patient has become a victim of medical identity theft. This hypothetical situation creates concern for the patient because their once-accurate medical records now contain erroneous information that may negatively affect the patient in the future. The patient may also receive bills for services they never received or requested. This patient may want to bring a lawsuit against the hospital to recoup their expenses and correct their medical records.

Courts offer no remedy for victims of medical identity theft, despite the pervasiveness of the problem. Because the patient-victim has suffered no "actual damage," the patient cannot file a lawsuit.[155] Courts have defined the "actual harm" requirement in various ways. In *Forbes v. Wells Fargo Bank*,[156] the court rejected the plaintiffs' claims of negligence because "the personal time and money spent . . . 'was not the result of any present injury, but rather the anticipation of future injury that has not materialized.'"[157] Other courts have said that to establish damages, the injury must be "actual or imminent, not conjectural or hypothetical."[158] Another hurdle plaintiffs face is establishing a breach of duty.[159] If the provider believes that it provided care to the patient, the provider did not breach its duty to provide said care.[160]

One recent way that some plaintiffs attempt to circumvent this hurdle is by bringing an individual negligence claim using HIPAA as a guidepost for the standard of care.[161] HIPAA sets requirements that healthcare providers must follow when handling personal information; if a plaintiff can show that a provider violated a

litigation [https://perma.cc/96ZJ-2K48] (describing how the "actual or imminent" harm requirement to move forward with litigation is an impossible hurdle that many plaintiffs are unable to overcome (citing Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 6 (D.D.C. 2007))).

155. Nahra, *supra* note 154.

156. Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006).

157. Nahra, *supra* note 154 (quoting *Forbes*, 420 F. Supp. 2d at 1021).

158. *Randolph*, 486 F. Supp. 2d at 6. In this case, a laptop containing the plaintiffs' personal information—belonging to an employee of defendant—was stolen. The plaintiffs claimed that identity theft would result and could lead to damages. *Id.* at 2. The court reasoned that damages cannot "amount to mere speculation that at some unspecified point . . . [plaintiffs] will be the victims of identity theft." *Id.* at 8.

159. *See generally* Nahra, *supra* note 154.

160. *Id.*

161. *Id.* (citing Acosta v. Bynum, 638 S.E.2d 246, 250–51 (N.C. Ct. App. 2006)).

requirement established by HIPAA, then the plaintiff may have a cause of action against the provider.[162]

The clearest case that illustrates the use of HIPAA to establish a negligence claim is *Acosta v. Bynum*,[163] where a psychiatrist let an office manager access patient records "that were then used to cause harm to a patient."[164] The court allowed for HIPAA to set the standard of care; thus, the plaintiffs only needed to show that that provider violated the standard of care under HIPAA.[165] Victims may still need to establish actual damages, but at least the *Acosta* standard provides a framework for victims to use in a private cause of action.[166]

Unfortunately, the more recent decision in *Clapper v. Amnesty International USA*,[167] has made it difficult for plaintiffs to succeed in claims of medical identity theft by stopping their claim before it can begin.[168] The court stated that the plaintiffs did not have standing to challenge the constitutionality of the Foreign Intelligence Surveillance Act because the plaintiffs' injury was merely hypothetical, not "certainly impending."[169] This case is analogous to data-breach cases because in both situations a plaintiff seeks to recover for an injury that could happen to the plaintiff because the risk of theft of the plaintiff's personal identifying information.[170] The "certainly impending" requirement to establish standing would eliminate almost the entirety of medical identity-theft cases resulting from a data breach.[171] This elimination would occur because it is nearly

162. *Id.*

163. Acosta v. Bynum, 638 S.E.2d 246 (N.C. Ct. App. 2006).

164. *Id.* at 253; Nahra, *supra* note 154.

165. Nahra, *supra* note 154.

166. *Id.*

167. Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

168. *Id.* at 401–02 (2013). This case involved several organizations that brought a suit challenging the constitutionality of section 702 of the Foreign Intelligence Act. *Id.* at 406–07. The act authorized the Director of National Intelligence and the Attorney General to conduct surveillance on individuals outside the United States and individuals who were non-U.S. citizens. *Id.* at 401.

169. *Id.* at 401–02.

170. *Id.* Previously in data breach cases, a plaintiff could recover if there was a "substantial risk" that a harm would occur as a result of the breach and exposure of personal information. *Id.* at 441 n.5. In *Clapper*, there had been no misuse of any information and only a possibility of future misuse of personal information. *See id.* at 401–02.

171. *See id.* In most data breach cases, a plaintiff has not yet suffered "actual" damage. Damages only result once an individual's stolen identity is fraudulently used by another. *Compare* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010)

impossible to determine whether a patient's information was taken.[172] Individuals whose personal identifying information was vulnerable during a data breach would not know whether their information was stolen until a third party used the individual's information.[173]

In most cases of a data breach, a victim is not aware of any specific use of their personal information for quite some time.[174] This delay makes it especially difficult to prove that the data breach will, in fact, cause an injury.[175] Accordingly, considering the data breach itself as the injury for which the plaintiff requires compensation makes the most sense.[176]

Some district courts have used the "substantial risk" standard when determining whether a plaintiff has established an injury for

(holding that the increased future risk of identity theft resulting from a stolen laptop containing names, addresses, and social security numbers of 97,000 employees was sufficient to establish Article III standing), *and* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (holding that an increased future risk of harm is sufficient to confer Article III standing), *with Clapper*, 568 U.S. at 401 (stating that an objectively reasonable likelihood that a respondents communications could be acquired at some point in the future was too speculative to satisfy the requirement that threatened injury be "certainly impending"), *and* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (holding that allegations of possible future injury stemming from a data breach were not sufficient to satisfy Article III standing because the threatened injury was not "certainly impending").

172. There is no way for an individual to know whether their information was taken during a data breach because although the thief may have had access to all the information, they may have only taken a portion. *Clapper*, 568 U.S. at 411 (citing Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644, 655–56 (6th Cir. 2007)) ("[C]oncluding that plaintiffs who lacked evidence that their communications had been intercepted did not have standing to challenge alleged NSA surveillance.").

173. The alert generally takes the form of an incorrect entry in a medical record or an erroneous bill for services the individual did not receive. The Court did not find an injury-in-fact to exist when a "speculative chain of possibilities" did not establish that "potential injury is certainly impending or is fairly traceable." *Clapper*, 568 U.S. at 414.

174. *See* Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 399 (2014) (discussing cases "in which the plaintiffs' information has been accessed but that information has not been used to open bank accounts, make unauthorized purchases, or otherwise harm the plaintiffs").

175. *Clapper*, 568 U.S. at 409.

176. *See* Cease, *supra* note 174, at 399 (explaining that even when plaintiffs' stolen information has not yet been used to their detriment, plaintiffs are harmed in other ways such as "incurring costs for credit-monitoring services, [and] paying the costs of cancelling and receiving new bank cards").

which they are owed recovery.[177] The Court in *Clapper* noted that even if courts applied the "substantial risk" standard, plaintiffs would have a hard time demonstrating that the possible future injury was not too attenuated.[178]

In a note examining the effects of *Clapper*, Claire Wilka argued that the holding —requiring that the substantial risk of future harm be certainly impending—should not apply when there is a threat of future medical identity theft following a data breach.[179] Wilka also argued that *Clapper* did not involve a data security breach and that courts should hold medical information compromised in a breach to an elevated standard above that of financial information.[180] Although Wilka's arguments are persuasive, courts have consistently dismissed cases for lack of standing when there is a data breach compromising personal medical information.[181]

Requiring an injury-in-fact in these situations eliminates almost any claim that a victim could bring. The injury-in-fact requirement compels victims to wait around and monitor all activity—which is impossible—for fraudulent usage of their personal information.[182] Such a requirement does not allow a victim to have peace of mind or to receive compensation for the act that allowed their personal information to be available and vulnerable to theft in the first place.[183] To address this problem, Wilka advocates for the use of the "substantial risk of harm" standard, which would benefit victims of data breach by allowing plaintiffs to establish standing before their information is misused.[184] A data breach of personally identifiable medical information could most likely satisfy the substantial risk of

177. Claire Wilka, Note, *The Effects of* Clapper v. Amnesty International USA*: An Improper Tightening of the Requirement for Article III Standing in Medical Data Breach Litigation*, 49 CREIGHTON L. REV. 467, 468 (2016) (stating that courts have noted that "because *Clapper* did not overrule the substantial risk line of cases, plaintiffs can establish standing if there is a substantial risk that the harm will occur").

178. *Clapper*, 568 U.S. at 441 n.5 ("Plaintiffs cannot rely on speculation about 'the unfettered choices made by independent actors not before the court.'" (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 562 (1992))).

179. *See* Wilka, *supra* note 177, at 480.

180. *Id.*

181. *Id.* at 472–73; *see, e.g.*, Peters v. St. Joseph Services Corp., 74 F. Supp. 3d 847 (S.D. Tex. 2015); *In re* Horizon Healthcare Services, Inc. Data Breach Litigation, No. 13-7418, 2015 WL 1472483 (D. N.J. March 31, 2015).

182. Wilka, *supra* note 177, at 470–71.

183. *Id.*

184. *Id.* at 487.

harm standard because the entity allowed the person's identifiable information to be at risk.[185] Since medical information is currently the most sought-after identity information, a substantial risk exists that someone has stolen any available information and will use it in the future.[186]

An obvious issue exists in determining what is considered a "substantial risk" of harm versus what is a "certainly impending" harm.[187] Courts have not defined the two terms or their respective distinctions.[188] Further, some critics have argued that the threat of identity theft possibly occurring is not enough to be considered a substantial risk.[189] However, Wilka argues that judicial intervention is necessary for data breaches of medical information because of the severity of the crime and because victims are left without recourse until they can prove a fraudulent use of their medical information has occurred.[190]

Unfortunately, numerous district courts have relied on the holding in *Clapper* to dismiss data breach claims for lack of standing.[191]

185. *Id.*

186. Medical information is the most profitable form of stolen identity information. McMahon, *supra* note 50, at 632–33 ("[T]he risk of suffering a penalty is well worth the reward for a potential thief."). Medical records fetch a higher price on the black market than financial information because of the versatility in the ways in which third parties can use medical information to impersonate an individual. Laura Shin, *A Decentralized U.S. Health System, Increasing Digitization of Records, and Demand in the Black Market are Fueling a Surge in Thefts*, FORTUNE (Oct. 19, 2014), http://fortune.com/2014/10/19/medical-identity-theft [https://perma.cc/UUC9-DBLH]. Medical information often contains a complete list of personal identifying information, such as a name, birth date, social security number, credit card information, and likely information on physical characteristics. *Id.* Different parts of the stolen medical information can be sold to different parties wishing to use various parts of the file for their unique needs. *Id.*

187. *See* Wilka, *supra* note 177, at 488–89.

188. *Id.* at 488.

189. *Id.* at 488–89.

190. *See id.*

191. *Id.* at 482; *see also* Peters v. St. Joseph Servs. Corp, 74 F. Supp. 3d 847, 854 (S.D. Tex. 2015) (finding that the representative of a class action lawsuit did not have standing because future injuries asserted by plaintiff were speculative and hypothetical); Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) (finding that plaintiffs did not establish a certainly impending injury-in-fact and dismissing the case).

## IV. SUGGESTIONS FOR PREVENTING IDENTITY THEFT

Over the years, several sources have suggested methods to prevent medical identity theft in the first place and how to improve the process of correcting a victim's medical record. One suggestion was put forth by Katherine Sullivan and states that making the prevention of medical identity theft a condition of licensure or accreditation would incentivize healthcare providers to better protect patient information.[192] Sullivan also analyzes a recommendation to amend HIPAA's privacy policy.[193] Another suggestion, made by Stanley Ball, recommends that the federal government implement a policy modeled after Ohio's law on data breach notification and expand the policy to cover healthcare providers.[194] Yet another suggestion was made by Thomas Clifford and calls for the adoption and standardization of Health Information Exchanges, along with heavier regulations on electronic medical records.[195]

### *A. Sullivan's Suggestions*

Sullivan suggests "mak[ing] the prevention of medical identity theft a condition of licensure or accreditation" for healthcare providers.[196] She argues that the safety goals of the Joint Commission—an independent not-for-profit entity that accredits hospitals and healthcare providers[197]—should be recast to include "occurrences of medical identity theft as of the Joint Commission's 'never events.'"[198] Sullivan next argues for technological innovations such as increased patient identification and limiting each employee's

192. Sullivan, *supra* note 47, at 675.

193. *Id.* at 677.

194. *See generally* Ball, *supra* note 21, at 112 (recommending many amendments to Ohio's law including expansion to medical providers).

195. Clifford, *supra* note 53, at 65.

196. Sullivan, *supra* note 47, at 675.

197. *See generally About the Joint Commission*, JOINT COMMISSION http://www.jointcommission.org/AboutUs [https://perma.cc/LCP5-K8LS].

198. Sullivan, *supra* note 47, at 676. The Center for Medicare and Medicaid Services (CMS) has a list of "never events" that are occurrences of egregious medical error that are not reimbursable by the federal government. *See* Press Release, Center for Medicare and Medicaid Services, Eliminating Serious, Preventable, and Costly Medical Errors-Never Events (May 18, 2006), https://www.cms.gov/newsroom/fact-sheets/eliminating-serious-preventable-and-costly-medical-errors-never-events [https://perma.cc/6MC5-B2ND].

access to medical records.[199] The most practical suggestion Sullivan makes is amending HIPAA's current privacy policy to allow a private cause of action against healthcare providers and to strengthen a victim's right to view and amend their healthcare records.[200] Allowing a private cause of action against healthcare providers would give victims a way to be reimbursed when identifying the individual thief is impossible.

The final suggestion that Sullivan proposes is to create a "Health Care History Report," much like the current Fair and Accurate Credit Transactions Act (FACTA) report.[201] Individuals would receive free access to an annual report that would contain any and all medical services that were related to the individual's social security number.[202] Although an individual would need to request the yearly report, the individual would receive the report at no cost.[203] Similar to the FACTA report, this system would also allow an individual to place a fraud alert or a hold on their report, which would notify the individual if any changes were made or if any health services were requested.[204] Sullivan explains that although a "Health Care History Report" would provide the most protections for victims, implementing this system in practice would be extremely difficult.[205]

199. Sullivan, *supra* note 47, at 676.

200. *See id.* at 677–78. Subjecting healthcare providers to private causes of action could incentivize providers to establish stricter policies to prevent medical identity theft in the first place. *Id.* at 678. A victim already has the legal right to view and amend their medical records if they request, put forth in a clarification by the HHC and the FTC. *See* FTC, *supra* note 91. However, having this right specifically stated in the Privacy Rule of HIPAA may make it clearer to providers.

201. S*ee* Sullivan, *supra* note 47, at 678. FACTA is an amendment to the Fair Credit Reporting Act that Congress added in 2003 to protect consumers from identity theft. *See generally* Fair and Accurate Credit Transactions Act, Pub. L. No. 108-159, 117 Stat. 195215 (2003). This act gives consumers the right to obtain one free credit report a year from credit reporting agencies. *Id.* FACTA also includes a section that lets consumers place fraud alerts on their credit files. *Id.*

202. Sullivan, *supra* note 47, at 678–79.

203. *Id.* at 679.

204. *Id.*

205. *Id.* Because there are too many agencies in charge of medical records, it would be impossible to have one aggregated system like the one under FACTA. *Id.* at 679–80. There is also the issue of the cost to upkeep such a system. *Id.* at 680. Sullivan explores further options for how to finance this report in the remainder of her note and comment. *Id.*

### *B. Ball's Suggestion*

Stanley Ball made another suggestion in his note, *Ohio's "Aggressive" Attack on Medical Identity Theft*.[206] In his note, Ball argued that the federal government should implement a system similar to the Ohio system—expanded to cover healthcare providers—to combat cases of medical identity theft.[207] Specifically, Ball argued that the Ohio legislature should expand its data-breach notification law to cover healthcare providers—specifically, that healthcare providers in Ohio should not have any exceptions to notifying patients when a data breach occurs; data breach legislation should require that healthcare providers destroy patient records when disposing of them; and victims of medical identity theft should have a mechanism to collect monetary penalties from healthcare providers who do not adhere to this legislation.[208]

Ohio's data-breach law requires that businesses notify Ohio residents of any data breaches if the following conditions are met: (1) a business discovers or is notified of a breach to its information system; (2) the business knows or reasonably believes that an unauthorized person accessed and acquired an Ohio resident's personal information; and (3) business reasonably believes that the access and acquisition of the Ohio residents information creates a material risk of identity theft or other fraud.[209]

Unfortunately, Ohio expressly decided to not broaden this legislation to include the protection of an individual's health information.[210]

### *C. Clifford's Suggestions*

Thomas Clifford analyzed Ball's proposal in his article *Provider Liability and Medical Identity Theft: Can I Get Your (Insurance)*

206. Ball, *supra* note 21, at 111.

207. *See generally id.* (arguing that the federal government could benefit from a system like Ohio's, which requires providers to notify individuals when there has been a data breach that could affect their information and penalizes institutions for failing to provide this notification).

208. *Id.* at 113. Four proposals are set out in Ball's note. *Id.* Disposing of medical data properly is especially important to combat medical identity theft because Ball explains that careless document disposal persists. *Id.* at 140.

209. OHIO REV. CODE § 1349.19(B)(1) (2007).

210. Ball, *supra* note 21, at 133.

*Number*?[211] Clifford found that Ball's "recommendation that the state law handling patient data protection should adopt more consumer remedies for breach of personal medical information is strong."[212] Clifford went on to explain that it is important for citizens to have some way of recovering monetary damages in instances of medical identity theft.[213]

Additionally, Clifford provided several new recommendations for ways the government could better protect patients.[214] The first recommendation was "the widespread adoption and standardization of Health Information Exchanges (HIEs), alongside regulation for electronic medical record interoperability."[215] Clifford argued that HIEs provide immense benefit to patients because HIEs aggregate every patient's medical records; therefore, any healthcare provider can access a patient's complete medical record.[216] However, Clifford noted that HIEs have limitations because HIEs consist of a variety of records from various medical institutions, so any incorrect information can be easily duplicated and circulated faster than it otherwise would.[217]

Although HIE's may be helpful in some situations for easier access to information from all healthcare providers, implementing this system for the storage of all records may be too difficult.[218] However, Clifford argued for a standardization of all medical record

211. Clifford, *supra* note 53, at 59–60.

212. *Id.* (quoting Ball, *supra* note 21, at 133).

213. Clifford, *supra* note 53, at 59–60.

214. *Id.* at 65.

215. *Id.* HIEs are organizations that collect all electronically stored information, such as patient data, in one place and allow for the sharing of that information between providers. *Id.* at 57. The American Medical Association is an advocate of utilizing HIEs for the sharing of medical information. *Id.* HIEs could eventually be morphed into personal health records (PHRs) which are "personal collections of health information that are owned and controlled by the patient." *Id.* at 67.

216. *Id.* at 57.

217. *Id.* If a thief uses an individual's identity to receive medical treatment under the victim's name, the provider will enter that medical care into the HIE under the victim's name and health history, making the identity misuse much more difficult to catch before it is circulated. *Id.*

218. *Id.* at 65–66. Every healthcare provider stores patient data differently. Some use open-ended questionnaires, in which the doctor fills in a blank after questions such as age, height, symptoms, diagnosis, etc. Other providers use checklists that list possible answers and physicians simply check off the ones that apply. *Id.* at 66.

keeping in healthcare provider practices.[219] Requiring all healthcare providers to store their data in a uniform format would allow for an accurate HIE system and for all healthcare providers to have the same access to information.[220] Clifford further argued that the federal government should require that HIEs include a system that allows patients to request copies and amend their total record.[221]

Other individuals who have researched medical identity theft argue that there should be a better system of admitting individuals at the front door of a healthcare provider's office to prevent the theft from occurring in the first place.[222] The amount of individual cases of medical identity theft would likely decrease as a result of requiring individuals to present a driver's license or passport before receiving healthcare service.[223] However, this requirement hardly addresses the fraud rings that perpetrate mass cases of medical identity theft.[224]

These proposals, while helpful, do not focus on relieving victims of medical identity theft from the responsibility of researching and resolving their claims in some way.[225] A more patient-protective and efficient proposal would be to require healthcare providers to be responsible for researching and resolving claims of medical identity theft or medical identity fraud. Healthcare providers are in the best

219. *Id.* at 66; s*ee also AMA Calls for EMR Standardization to Ease Physician Use*, FIERCE HEALTHCARE (June 23, 2011), https://www.fiercehealthcare.com/ehr/ama-calls-for-emr-standardization-to-ease-physician-use [https://perma.cc/FPL7-4GG3].

220. Clifford, *supra* note 53, at 66 (explaining that the financial impact of such a system would save the healthcare industry an estimated eighty-one billion dollars).

221. *Id.* Having a uniform system where patients can amend any of their medical records would be a significant convenience for patients. *Id.* Currently, patients must contact each entity that has any health records and amend each record individually. *Id.*

222. Dixon, *supra* note 18, at 13. In theory, a more thorough intake of patients would uncover the lone fraudster who has stolen someone's license or social security number. *Id.* Healthcare providers may be able to stop some smaller forms of medical identity theft by requiring patients to present photo identification. *Id.*

223. *Id.* at 7. Some hospitals have already implemented these types of procedures after becoming aware of incidents of medical identity theft at their institutions. *Id.* One such institution was the University of Connecticut Health Center, which began checking patient's driver's licenses after a case of medical identity theft. *Id.*

224. *Id.* at 53. Mass cases of medical identity theft may occur when a ring of thieves is systematically "billing and changing medical files without ever stepping foot in the healthcare provider's office or seeing a single patient." *Id.*

225. *See* Clifford, *supra* note 53, at 61; *see also* Ball, *supra* note 21, at 127–28; Sullivan, *supra* note 47, at 647.

position to research and resolve a claim of medical identity theft with a limited expenditure of cost and time. Healthcare providers should not require victims to resolve their own claims of theft and fraud that occurred because of a healthcare provider's negligence in securing their patient's personal identifying information. As Clifford points out:

> Patients whose personal data has been breached, and who subsequently sustained harm, such as a loss of medical identity, should be able to receive fair compensation, including, but not limited to, the actual process of restoring one's identity security, accuracy of medical records, and credit rating. In particular, they should be reimbursed for time and expenses related to interacting with the credit agencies and to remove fraudulent charges.[226]

At the very least, patients should have an avenue to collect the monetary expenses they have incurred in trying to resolve and correct their medical records.

## V. SHIFTING THE INVESTIGATIVE BURDEN TO PROVIDERS

It is almost impossible for victims of medical identity theft to investigate and correct the issue on their own. Unfortunately, HIPAA creates administrative roadblocks that victims cannot navigate. The very purpose of HIPAA is to prevent unqualified third parties from gaining access to a patient's personal information.[227] However, healthcare providers incorrectly believe that HIPPA denies access of information to a victim of identity theft who seeks information surrounding the care they supposedly received, even though the victim received the bill and the provider recorded care under the victim's medical history.[228]

Healthcare providers must be required to develop their own institutional policies to address claims of medical identity theft.[229] Having such policies in place would educate all members of the healthcare institution on the importance of prevention and detection of medical identity theft.

226. Clifford, *supra* note 53, at 63 (responding to Ball's proposal for more stringent data protection measures).

227. *See generally* Sullivan, *supra* note 47, at 660–62 (explaining that because patients are unable to view their fraudulent records due to healthcare providers' fear of violating HIPAA, victims are often unable to solve claims of medical identity theft).

228. *Id.*

229. *See generally* Mancini, *supra* note 148, at 901 (analyzing how emergency room providers' awareness of medical identity theft is crucial to prevention).

Because an identity thief's medical records are also protected under HIPAA, significant confusion exists among healthcare providers about whether HIPAA prohibits the release of a victim's medical records to the victim.[230] Many providers believe that releasing medical records—containing information on services or care rendered to an individual using the victims stolen identity—to the victim violates HIPAA.[231] There is so much confusion on this issue that in 2015 the chairs and ranking members of the Senate Committee on Health, Education, Labor, and Pensions, and the Senate Committee on Finance sent a letter to the Department of Health and Human Services (HHS) requesting clarification.[232] The FTC and the HHS previously attempted to address and answer these issues in 2011[233] and developed a pamphlet to aid providers in resolving claims of medical identity theft and in responding to victim's concerns.[234] The pamphlet states:

> The HIPAA Privacy Rule gives people the right to copies of their records maintained by covered health plans and medical providers. . . . Some medical providers and health plans believe they would be violating the identity thief's HIPAA privacy rights if they gave victims copies of their own records. That's not true. Even in this situation patients have the right to get copies of their records.[235]

230. Adam H. Greene, *Confusion Continues Over Medical Identity Theft Victim Rights under HIPAA*, PRIVACY & SECURITY L. BLOG (Dec. 1, 2015), http://www.privsecblog.com/2015/12/articles/healthcare/confusion-continues-over-medical-identity-theft-victim-rights-under-hipaa [https://perma.cc/8V6F-JD6P] (illustrating that many healthcare providers hold this belief because providers are essentially allowing an individual to see another patient's records, even though those records are under the individual's name).

231. *Id.*

232. *Id.* The letter stated that "[w]hile patients have the right to view and request corrections to their medical records under the . . . [HIPPA] Privacy Rule, there is widespread confusion about how this rule applies in the case of a thief's information being comingled with that of his or her victim's" and that the "Ponemon Institute reported that nearly one in five victims of medical identity theft were refused access to their medical records 'due to laws protecting the privacy of the identity thief.'" *Id.*

233. *Id.*

234. FED. TRADE COMM'N, MEDICAL IDENTITY THEFT: FAQS FOR HEALTH CARE PROVIDERS AND HEALTH PLANS (2011), https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf [https://perma.cc/X2U2-8KHR].

235. *Id.* at 4–5.

Despite the FTC and the HHS's attempt to resolve the confusion plaguing healthcare providers, confusion remains. The letter requesting additional clarification in 2015 highlights this lingering confusion.

Sullivan explored how the creation and handling of medical records creates an impossible maze for victims of medical identity theft to navigate.[236] Sullivan argued that most healthcare billing and recording systems have not been updated as the financial systems have, and so have not evolved with the increasingly complicated diagnostic technology of healthcare.[237] Sullivan also examined the difference between financial transaction processing and medical claims billing, focusing on which process is more protective of patients' medical information.[238]

There are currently very few legal remedies that a victim of medical identity theft can pursue.[239] With so much confusion surrounding how to handle victims' medical record requests, the safest and most efficient way to resolve claims is to have the provider take responsibility for researching and resolving claims of medical identity theft and to cover all fees associated with any necessary corrections. When hospitals themselves are not allowing patients access to their medical records for fear of a HIPAA violation against the thief's rights, requiring the victim to attempt to remedy the situation does not make sense.

Providers and some scholars argue that a burden shift is not appropriate because too much responsibility would fall on small,

236. Sullivan, *supra* note 47, at 653–54.

237. *Id.* at 654. The culmination of laboratory work, pharmacists, specialists, and third-party diagnostic services all required for one doctor visit results in multiple people touching a patient's records and distributing those records to multiple institutions outside of the primary healthcare provider's office. *Id.* Healthcare providers (or the patient) must also send a detailed record of each service to the patient's insurance company, who then creates an additional record. A hospital stay requires granting even more individuals access to view and to change medical records. *Id.*

238. *Id.* at 655.

239. *See* Clifford, *supra* note 53, at 58–67 (offering suggestions to prevent medical identity theft); Sullivan, *supra* note 47, at 674–81 (offering suggestions to detect medical identity theft and regulate patient information in the healthcare industry). *See generally* Dixon, *supra* note 18, at 8–9 (explaining the few ways that victims of medical identity theft can report their cases).

independent practitioners.[240] However compelling this argument may be, it does not outweigh the potential benefits of a healthcare system that takes responsibility for protecting patients' privacy.

In addition to requiring healthcare providers to investigate any claims of medical identity theft, laws should also require healthcare providers to use electronic records. Electronic records, when handled correctly, allow for a centralized record keeping system.[241] Having a centralized system makes it easier for healthcare providers to confirm and correct patients' medical records.[242]

The former attorney general of California recognized medical identity theft as the "privacy crime that can kill"[243] and developed a guide for addressing the problem. The guide offers several recommendations to healthcare providers when responding to claims of medical identity theft, including "[i]mplement[ing] an identity theft response program with clear written policies and procedures for investigating a flagged record," and "[t]rain[ing] staff in all relevant departments on these policies and procedures."[244] Additionally, the guide states that the "responsibility for preventing, detecting and mitigating medical identity theft lies primarily with the healthcare industry; although patients can also help."[245] The purpose of the California attorney general's guide was to offer ways to help healthcare providers and related organizations develop better practices that will "promote and protect individual privacy right."[246]

240. Clifford, *supra* note 53, at 65 (explaining that the burden placed on small, independent practitioners does create a problem, but that the problem may not outweigh the need to protect patient identity).

241. Dixon, *supra* note 18, at 9–10. If not handled correctly, an electronic record keeping system could make stealing patient data even easier for thieves. *Id.* at 10. "Digitized information is much more portable and lends itself to rapid transmission." *Id.* Because an electronic system also allows for the easy perpetuation of incorrect data, electronically connected healthcare systems could "percolate [incorrect data] through a nationwide system." *Id.*

242. *See id.*

243. HARRIS, *supra* note 43, at i (laying out suggestions and recommendations for healthcare providers in California to follow when addressing claims of medical identity theft).

244. *Id.* at iii. Harris also recommended "[o]ffer[ing] patients who believe they may be victims of identity theft a free copy of the relevant portions of their records to review for signs of fraud." *Id.*

245. *Id.* at 2. This statement is in opposition to our current system where patients are responsible for resolving their own claims.

246. *Id.* at 3.

States and the federal government could use the guide as a blueprint for mandating a process for dealing with cases of medical identity theft. The guide advocates implementing a follow-up procedure for patients claiming that their bills include medical information that does not belong to them.[247] This course of action first involves gathering all of the necessary patient information. Once that is completed, the healthcare provider places the patient's financial obligations on hold while a team investigates the issue.[248]

If the team determines that a medical identity theft occurred, clear policies should be in place and followed for handling the corrupted records.[249] Healthcare providers must make corrections to victims' records in the appropriate manner based on the particular circumstances.[250]

Some providers and scholars object to this burden shift, reasoning that the responsibility placed on providers would be too great.[251] This is mostly a financial argument, claiming that smaller providers will not be able to meet the financial requirements of a burden shift and will no longer be profitable.[252] This is a valid argument and one that merits brief analysis. Even though this burden shift will be financially taxing, it will be more cost-effective in the long

247. *Id.* at 9–10. For example, healthcare providers could use a form with pre-determined questions when interviewing a patient for details about the complaint. *Id.* at 9.

248. *Id.* In cases where the individual is not a patient, the provider should still investigate the claim in the same manner. *Id.* at 9–10. If the provider determines that medical identity theft occurred, then the provider should notify the individual and give the individual thorough information on how to proceed. *Id.* at 10.

249. HARRIS, *supra* note 43, at 5 (setting forth suggestions and recommendations for healthcare providers in California to follow when addressing claims of medical identity theft).

250. *Id.* This could mean many things: removing the incorrect information; leaving the information but noting clearly that it does not belong to the victim; creating a new file for the victim; notifying all relevant parties; and notifying the victim of the steps taken to correct the issue. *Id.* Further suggestions include creating separate files labeled "medical identify theft." *Id.* Ideally, this would allow for moving the incorrect information contained in a victim's file to a new, centralized location. *Id.*

251. Clifford, *supra* note 53, at 65 (reasoning that small healthcare facilities would face an undue financial burden in implementing policies and procedures and possibly employing additional personnel to research and resolve medical identity theft claims).

252. *Id.* This burden may not be affordable for some smaller providers to implement upfront. *Id.*

run.[253] Placing the responsibility on providers to resolve claims would make the patient intake process more effective regarding identity theft prevention.[254] Providers would exercise more care when investigating claims of medical identity theft to avoid the cost of resolving future claims.[255] Clifford echoed this idea in advocating for a liability shift from patients to providers.[256]

Placing the liability on healthcare providers would incentivize better practices to determine patient identity.[257] From an economic standpoint, Clifford argued that providers should bear the burden.[258] Economic efficiency determines liability for negligence and strict liability in cases where the questions are "who can most efficiently reduce the risk of this problem . . . [and]...who benefits from this risk and therefore should bear the cost?"[259] Much like the credit card industry—which has been required to establish policies to prevent and detect financial identity theft through recognizing unauthorized uses of personal information—healthcare providers should be required to implement similar systems.[260] If healthcare providers are legally required to bear the financial risk, they will be far more likely to work to prevent medical identity theft in the first place.[261]

## VI. CONCLUSION

Medical identity theft is a crime that leaves victims with financial losses, emotional stress, and the possibility of incorrect medical records. Because this crime is so personal, it is extremely important

253. *See generally* Sullivan, *supra* note 47 (calling for a better intake system in healthcare facilities). Providers would avoid having to pay out services that were fraudulently received if they develop the proper systems to avoid providing the service to thieves in the first place.

254. *See id.* Providers would not want the responsibility of paying for services of individuals who claim their medical identities stolen and did not receive the services given.

255. *See id.*

256. Clifford, *supra* note 53, at 61.

257. *Id.* at 63.

258. *Id.* at 61–63.

259. *Id.* at 61 (quoting Jason S. Johnston, *Punitive Liability: A New Paradigm of Efficiency in Tort Law*, 87 COLUM. L. REV. 1385, 1393 (1987)).

260. *See id.*

261. *Id.* at 63. The financial risk entails the amounts that are required for the research and resolution of claims of medical identity theft. Clifford recommends using specific statutes to "ensure that patients receive the most protection in the unfortunate event of medical identity theft." *Id.* at 62.

that victims have a method to correct their records and report any claims. With the current system, it is nearly impossible for victims to resolve claims on their own.[262] Providers feel as though they are not allowed to provide victims with their own medical records for fear of violating HIPAA's privacy policies.[263] To repair this system, healthcare providers must be the ones to research and resolve claims of medical identity theft because they are in the best position to efficiently resolve these issues and protect patient information.[264]

Thus, by shifting the burden to healthcare providers, claims would be more efficiently resolved, and patients' information will be corrected faster, resulting in fewer complications related to incorrect medical information in patient records.[265]

262. Sullivan, *supra* note 47, at 653–57 (explaining the roadblocks that a victim of medical identity theft faces when trying to research and amend their medical records). Most of the problems are due to healthcare providers' misunderstanding of HIPPA regulations. *Id.* at 662; *see also* Greene, *supra* note 230. Healthcare providers are mainly concerned that they will be in violation of HIPAA if they provide an individual with medical records after that individual has claimed that their identity has been stolen and that their records contain a service that they had never received. Clifford, *supra* note 53, at 53; Greene, *supra* note 230.

263. Greene, *supra* note 230.

264. Clifford, *supra* note 53, at 61–63.

265. *Id.* at 63.