Northwestern Journal of Law & Social Policy

Volume 12 | Issue 1 Article 2

Fall 2016

Provider Liability and Medical Identity Theft: Can I Get Your (Insurance) Number?

Thomas Clifford

Vol. 12, Issue 1 (2016)
Northwestern Journal of Law and Social Policy

Provider Liability and Medical Identity Theft: Can I Get Your (Insurance) Number?

Thomas Clifford

I. MEDICAL IDENTITY FRAUD: DEFINING THE PROBLEM

According to the U.S. Department of Health and Human Services, medical identity theft occurs when personal information is stolen and used to obtain medical care, buy drugs, or submit fake billings.[1] The consequences of medical identity theft are severe and typically take one of two forms: financial or medical.[2] Financial consequences are frequently the result of false claims being filed. False insurance claims can have dramatically adverse consequences, including fraudulent bills at times costing over $100,000.[3] The process of getting false claims removed from your credit history is long, arduous, and cumbersome.[4] With regard to medical consequences, serious fallout results from the inaccurate documentation of medical history.[5] With the proliferation of electronic health records, erroneous documentation is easily replicated and spread from one institution's database to another's.

This Comment analyzes the medical identity theft phenomenon through a variety of stages. Section II describes how medical identity theft happens, what happens to a patient after his or her information has been used to receive care, and includes statistics on the prevalence of medical identity theft. This section also covers the process of how criminals might obtain patient data, how they use the data, and how hospitals handle patient data. Section III focuses on analysis, looking at industry and government responses to medical identity theft. Additionally, this section reviews several proposed reforms to fight back against medical identity fraud, followed by several recommendations regarding the best measures to resolve medical identity theft. In particular, this Comment argues that economic analysis supports moving the de facto liability of medical identity theft from patients to providers. Further, this Comment argues that new technological developments can make this proposal more feasible than it was just a few years ago, and that developments such as health information exchanges can be utilized not only for patient health, but also for patient information protection.

---

[1] *Medical ID Theft/Fraud Information*, OFFICE OF THE INSPECTOR GENERAL U.S. DEP'T OF HEALTH & HUMAN SERVS., https://oig.hhs.gov/fraud/medical-id-theft/ (last visited Mar. 21, 2016).
[2] *Id.*
[3] Christie Aschwanden, *How to Protect Yourself From Medical Identity Fraud*, THE WASHINGTON POST (Feb. 3, 2014), http://www.washingtonpost.com/national/health-science/how-to-protect-yourself-from-medical-identity-fraud-a-first-step-dont-tweet-health-issues/2014/02/03/514aa192-876e-11e3-916e-e01534b1e132_story.html.
[4] *The Growing Threat of Medical Identity Fraud*, THE MEDICAL IDENTITY FRAUD ALLIANCE, 5 (July 2013), http://medidfraud.org/wp-content/uploads/2013/07/MIFA-Growing-Threat-07232013.pdf.
[5] *Id.*

Finally, Section IV places these recommendations and conclusions in the broader context of the healthcare industry.

II. The Current State of Medical Identity Theft

A. How It Happens

1. Stories from Victims

In 2002, seventeen-year-old Nikki Burton went to donate blood for her first time.[6] After presenting[7] for the donation, she was turned away without any explanation.[8] Burton, confused by the situation, decided to follow-up with the Red Cross headquarters.[9] There, she learned that the Red Cross barred her from donating because her Social Security number had been used to procure free treatment from a California AIDS clinic, despite Burton never having been to an AIDS clinic herself.[10] A thief had stolen her number, which allowed someone other than Burton herself to show up at the clinic to receive treatment.[11] Although the Red Cross no longer requires a Social Security number to donate blood, imagine the negative fallout if the Red Cross servers were breached and this false medical documentation was leaked to the public.[12]

In another case, a woman who was over six feet tall was scheduled to undergo bypass surgery but had a medical record that listed her height as just over five feet.[13] The error in her medical record existed because another patient had taken her identity and used it to receive medical care.[14] Because anesthetics and other medication dosage is prescribed based on patient height and weight, the difference could have had serious complications had it not been noticed and corrected before the surgery took place.[15]

In an even more alarming case, Linda Weaver, the owner of a horse farm in Florida, walked to her mailbox and found a bill for the amputation of her right foot, which was still attached to her leg![16] Upon contesting the charges with the hospital, and pointing out that she still had two feet, she found reluctance from the hospital to fix her record, and was told the bill was "her responsibility."[17] The hospital dropped her bill after she threatened litigation, but the trouble continued.[18] Her insurance refused to pay the bill

---

[6] Laura Shin, *Medical Identity Theft: How the Health Care Industry Is Failing Us*, FORTUNE (Aug. 31, 2014, 1:51 PM), http://fortune.com/2014/08/31/medical-identity-theft-how-the-health-care-industry-is-failing-us/.

[7] "Presenting" is a term used in medical settings to describe a patient's arrival at a hospital or clinic to be either be admitted or checked in, for either an inpatient or outpatient procedure, or for an appointment.

[8] Shin, *supra* note 6.

[9] Shin, *supra* note 6.

[10] Shin, *supra* note 6.

[11] Shin, *supra* note 6.

[12] Shin, *supra* note 6.

[13] Aschwanden, *supra* note 3.

[14] Aschwanden, *supra* note 3.

[15] Aschwanden, *supra* note 3.

[16] Lorelei Laird, *Federal Medical-Privacy Law Frustrates ID Theft Victims*, A.B.A. J. (Sep. 1, 2014, 9:10 AM), http://www.abajournal.com/mobile/mag_article/federal_medical-privacy_law_frustrates_id_theft_victims/.

[17] Sibile Morency, *Medical ID Theft Threatens Unsuspecting Victims' Lives*, ABC NEWS (Nov. 21, 2006), http://abcnews.go.com/Health/story?id=2668314.

[18] *Id.*

because she was not the one who received treatment, but the doctors also refused to drop the bill.[19] Soon, they sent the bills to collection agencies, and Weaver's credit score was ruined.[20] Even though she was told that the thief's medical history had been purged from Weaver's own insurance record, after receiving emergency care for a heart attack, she realized that false information persisted, and the nurse had assumed that Weaver had diabetes because of the medical information she had on file with the hospital.[21]

2. The Industry Numbers

According to the Medical Identity Fraud Alliance, medical identity fraud has been growing at a steady pace.[22] A three-year study of medical identity fraud in the United States by the Ponemon Institute, a group that offers privacy-related strategic counseling, estimated 1.42 million victims in 2010, 1.49 million in 2011, and 1.85 million in 2012.[23] Seventy-five percent of victims polled in this study reported financial consequences, and 20% indicated that their credit scores had suffered as a result of medical identity fraud.[24] Furthermore, 15% of victims incurred legal fees, and about 8% saw increases in their health insurance premiums as a result.[25] In March 2015, eleven employees of Blue Cross Blue Shield of Michigan were charged with using stolen insurance subscriber information from 5,000 patients to purchase $742,000 worth of merchandise from Sam's Club.[26] This is representative of an industry-wide problem and demonstrates the vulnerability of personal medicalinformation.

One of the reasons that medical identity theft is growing is because it is significantly more lucrative than traditional identity theft; a stolen Social Security number typically only sells for $1 on the black market, but a stolen medical identity typically sells for $50.[27]

3. Data Breach: How Criminals Access Victims' Personal Health Information

Criminals can gain access to individuals' medical identity in a variety of ways. A common method for getting insurance information is when a criminal persuades an individual to reveal his or her insurance information.[28] Often criminals will target senior centers or homeless centers to ask for Medicare numbers in exchange for $50.[29] Alternatively, criminals have established some more elaborate schemes to collect insurance information, such as inviting seniors to imitation "health fairs" that are rouses

[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *The Growing Threat of Medical Identity Fraud*, *supra* note 4.
[23] *The Growing Threat of Medical Identity Fraud*, *supra* note 4.
[24] *The Growing Threat of Medical Identity Fraud*, *supra* note 4.
[25] *The Growing Threat of Medical Identity Fraud*, *supra* note 4.
[26] Holly Fournier & Mark Hicks, *11 Charged in Blue Cross ID Theft, Fraud*, THE DETROIT NEWS (March 11, 2015), http://www.detroitnews.com/story/business/2015/03/10/charged-theft-blue-cross-subscriber-info/24711063/.
[27] *The Growing Threat of Medical Identity Fraud*, *supra* note 4.
[28] Aschwanden, *supra* note 3.
[29] Aschwanden, *supra* note 3.

to get seniors to disclose personal information.[30] In these "health fairs", criminals might take seniors' blood pressure, give them nutritional supplements, and then ask to see their Medicare cards.[31]

Sometimes, criminals are able to get patient insurance information simply because patients are either careless or do not understand the importance of keeping their medical information confidential.[32] Jennifer Trussell, an employee of the U.S. Department of Health and Human Services' (HHS) Office of the Inspector General (OIG) who has worked on medical identity theft investigations, has compared posting about a diagnosis on social media to posting an address along with the days someone will be away on vacation.[33] This is because a diagnosis makes it easier for someone to make false insurance claims that will not arouse suspicion.[34] For instance, if a criminal has someone's insurance information, and knows that the real insured consumer has diabetes, the criminal would know that making insurance claims for diabetes supplies would not likely raise the red flags that a claim associated with a totally new type of diagnosis would.[35]

More broadly, patients might become victims because others have been careless with their information, or because of vulnerabilities they could not have reasonably known about. HIPAA requires that HHS post all reported data breaches that affect 500 or more individuals.[36] In 2014, there were 289 reported data breaches by HIPAA-covered entities that affected 500 or more patients.[37] In 2015, there were 270 such breaches. As of November 2016, there were 261 in 2016.[38] These incidents include cases where the data breach occurred because of "hacking/IT incidents", improper disposal of data, data loss, theft, and unauthorized access of data, among other reasons.[39] Because HIPAA regulations govern a large subset of information, it is hard to say exactly which pieces of information were leaked, and how much of that information led directly to patient harm. However, some examples of data-storage locations that were breached include: paper, films, network servers, laptops, desktop computers, e-mail, and the broad category of any "other portable electronic device."[40]

Often, patients are the victims of those in whom they place the greatest amount of trust: their doctors.[41] In 1994, Debra Herritt learned this the hard way when she was reading the newspaper and came across the arrest of her psychiatrist, Richard Skodnek.[42]

---

[30] Aschwanden, *supra* note 3.
[31] Aschwanden, *supra* note 3.
[32] Aschwanden, *supra* note 3.
[33] Aschwanden, *supra* note 3.
[34] Aschwanden, *supra* note 3.
[35] Aschwanden, *supra* note 3.
[36] HIPAA is the Health Insurance Portability and Accountability Act: a statute governing how entities storing patient data must manage and protect that information. *See Instructions for Submitting Notice of a Breach to the Secretary*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html (last visited Mar. 20, 2015).
[37] *Breaches Affecting 500 or More Individuals*, U.S. DEP'T OF HEALTH & HUMAN SERVS., OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Jan. 24, 2016).
[38] *Id.*
[39] *Id.*
[40] *Breaches Affecting 500 or More Individuals*, U.S. DEP'T OF HEALTH & HUMAN SERVS., OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Mar. 20, 2015).
[41] Morency, *supra* note 17.
[42] Morency, *supra* note 17.

The psychiatrist would bill her for visits, then bill her insurance company for the same charges. He would also bill the insurance company for visits that never occurred, including visits for her children, who Skodnek never treated![43] Because insurance plans often cover many members of the family, this means families could be particularly lucrative victims for criminals perpetrating medical theft.

Regardless of how their information was stolen, victims can suffer a shocking impact from medical identity theft.[44] Thirty-six percent of medical identity theft victims incurred out-of-pocket costs, for which the average was $18,660; however, there are extreme cases where the costs exceeded $100,000.[45] Victims are blindsided when they receive hefty bills for care, or find out their Medicare accounts are maxed out.[46]

An even greater threat to patient identities may lie in publicly available information that allows a criminal to identify an individual's private information, then use it to pose as a consumer. For example, many public institutions have begun to release data to the public in hopes of the public mining those data for useful results.[47] Often, these data are "de-identified", which means that all information that could identify an individual patient is removed to protect the patient's identity.[48] Increasingly, however, computer programmers and data analysts have been able to link publicly available data to "de-identified" data to find out whom specific data represents.[49] They are able to establish this connection because many pieces of information that appear unrevealing are unique to a single person, and if these types of information are accidentally included in a set of "de-identified" data, they could be used to link certain information back to you.[50] For example, 87% of Americans have a unique combination of sex, birth date (including year), and zip code.[51] Further, the combination of city, birth date, and sex is unique for 53% of Americans, while the combination of county, birth date, and sex is unique for 18%.[52]

An example of the dangers in released information lies in a story from the Massachusetts government agency, the Group Insurance Commission (GIC), which in the mid-1990s released de-identified records that included summaries of every state employee's hospital visits.[53] These records were provided at no cost to researchers who had requested the files.[54] The GIC believed that the information had been de-identified

---

[43] Morency, *supra* note 17.
[44] Aschwanden, *supra* note 3.
[45] Aschwanden, *supra* note 3.
[46] Aschwanden, *supra* note 3.
[47] *See Divvy Data*, DIVVY, https://www.divvybikes.com/data (last visited Jan. 25, 2016). Divvy is a Chicago-based bike-sharing service that releases data on all trips taken with the company's bikes, in the hopes that policy makers, web developers, and designers will be able to use it for decision-making. Divvy uses the results of this open data project to produce information on which routes are most used and save their customers the most time.
[48] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html (last visited Nov. 16, 2014).
[49] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703–04 (2010).
[50] *Id.*
[51] *Id.* at 1705.
[52] *Id.* at 1719.
[53] *Id.*
[54] *Id.*

because it had removed fields considered to be explicit identifiers (e.g. name, address, Social Security number).[55] However, the data the GIC released still included information that could identify people indirectly—specifically, birth date, zip code, and sex.[56]

One enterprising graduate student purchased the complete voter rolls for Cambridge, where the governor lived. The voter rolls included the name, address, zip code, birth date, and sex for each voter.[57] Using this information, the graduate student was then able to combine it with the publicly available "de-identified" records from the GIC.[58] Six people in Cambridge shared the Governor's birth date, only three were men, and the governor was the only one in his zip code.[59] The researcher thereby identified the governor's health history, which included his diagnoses and prescriptions.[60] While this is an extreme case, because such extensive medical documentation has not been released regarding most patients (yet), it is easy to imagine criminals linking online information about consumers from disparate sources, then using that information to fraudulently gain access to healthcare treatment.

B. How Hospitals Collect Information

To understand how the actual use of patient information occurs, it is helpful to have a thorough understanding of hospital revenue cycle operations. For outpatient appointments, patients generally have their first interaction with a provider during the scheduling process.[61] For inpatient procedures, it might be during an initial scheduling process or upon the patient's arrival at the hospital. All of these initial provider encounters with a patient will include registration elements, collecting the patient's information such as the patient's name, date of birth, Social Security number, address, ethnic background, racial background, insurance information, billing address, and more.[62]

As a patient receives care, providers and nurses will document the patient's answers to medical history questions, generally recording the services provided as well as things like allergy information, descriptions of symptoms, diagnoses, procedure information, prescriptions, and potentially other data.[63] At the end of care, providers will record the services they provided, and send the charges to insurance companies for approval.[64] If the patient received care at a hospital, the patient will generally receive a separate set of hospital charges.[65]

After these charges are calculated, they are sent to a billing office where they are coded, and then sent out to insurance companies.[66] For surgeries, and other services with large charges that are scheduled well in advance, someone who works with the hospital

---

[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.* at 1720.
[60] *Id.*
[61] RONALD V. BUCCI, MEDICINE AND BUSINESS: A PRACTITIONER'S GUIDE 22 (2014).
[62] *Id.* at 23.
[63] *Id.* at 25.
[64] *Id.*
[65] *Id.*
[66] *Id.*

or provider will typically call the patient's insurance provider ahead of time to receive authorization to perform the procedure.[67].[68]

After the patient has received treatment, insurance payors will review the details, including diagnoses and procedures, make payments to the medical providers and the hospital.[69] Next, the insurance payor will send the patient an "Explanation of Benefits" statement (EOB) to notify them of what has been paid out and how it may affect the patient (such as through a deductible).[70] The hospital or medical provider will then send the patient a bill for any outstanding amount he owes that was not covered by the insurance claim.[71]

C. After Theft: Criminal Use of Medical Identity

After a patient's identity has been stolen, it might affect the patient at any number of points along the continuum of care described above. For example, a criminal might present the victim's insurance information at a hospital and request treatment for any type of care. Although the hospital may require a photo ID at the time a patient presents for treatment, healthcare has become exceedingly expensive, and the cost of a fake ID is far outweighed by the savings from free (stolen) medical treatment.

Alternatively, the patient's medical information may be stolen for reasons other than receiving medical care. Criminals will often seek a patient's medical information to submit false claims for care already received, either in conjunction with a criminal medical provider, or falsely posing as a medical provider.

D. After Theft: How Victims are Currently Expected to Respond.

After an individual realizes that he has been a victim of identity theft, his next move needs to be to mitigate the immediate effects, as well as correct the long-term effects, such as now having inaccurate medical records included in his medical history, and a potentially adverse effect to his credit rating.

A victim, in confusion and despair at the situation he faces, may want to turn to the authorities for assistance. Unfortunately, the government has multiple confusing websites that cross-reference each other and link to unusable material.[72] This leaves the victim in a state of uncertainty and confusion, causing further delay and making resolution to his identity security problems more difficult.

The HHS OIG website lists three subsections to address medical identity fraud: Deter, Detect, and Defend.[73] The "Defend" section simply recommends looking for unfamiliar or unusual charges on medical bills, and suggests calling the HHS OIG in the case of Medicare fraud, and the Federal Trade Commission (FTC) in the case of

---

[67] *Id*. at 24.
[68] *Id.*
[69] *Id.*
[70] *Report Healthcare Fraud: Explanation of Benefits*, BLUECROSS BLUESHIELD, http://www.bcbs.com/report-healthcare-fraud/explanation-of-benefits.html? (last visited Nov. 11, 2016).
[71] Bucci, *supra* note 61, at 24-25.
[72] *See Correcting Mistakes in Your Medical Records*, FEDERAL TRADE COMMISSION, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft#Correcting (last visited Mar. 10, 2016); *see also Medical ID Theft/Fraud Information*, *supra* note 1.
[73] *Medical ID Theft/Fraud Information*, *supra* note 1.

suspected misuse of someone's personal information.[74] The page then provides a list of five resources: (1) the HHS OIG hotline, (2) the Medicare Call Center, (3) a number to contact "local Senior Medicare Patrols who work locally to empower seniors to fight health care fraud and resolve errors," (4) the FTC's Identity Theft Hotline, and (5) a link to the World Privacy Forum's page on medical identity theft.[75] At the end of the HHS OIG page, there is a link to "Access OIG's Medical Theft Brochure."[76] This brochure is a PDF document that simply repeats all the information listed earlier on the page.[77] This circular set of information is ultimately unhelpful to anyone trying to resolve a medical identity theft issue.

The FTC webpage on medical identity theft is equally problematic. Its page on medical identity theft is part of a consumer information website focused more generally on privacy and identity violations, and repairing identity theft.[78] Although this page is in some ways more useful to the average American, as it more broadly covers any victim of identity theft, not just Medicare recipients who are victims of identity theft, the page is still rife with demonstrations of the barriers the victims must overcome, along with an organizational structure that might further confuse fraud victims.[79] The following confusing FTC webpage structure and jumbled presentation of information is indicative of the limited and insufficient solutions available to victims more generally.

The page begins with a section entitled "Detecting Medical Identity Theft," which recommends only the most basic pieces of advice, such as reading EOB statements from insurers to make sure that the claims paid match the care received.[80] They also offer advice like looking for signs of medical identity theft such as bills for medical services not received, calls from debt collectors about medical debts not owed, unrecognized medical collections notices on a credit report, notice that benefit limits have been reached, or denial of insurance because medical records show a condition that the insured does not have.[81]

The next section on the FTC's page is entitled "Correcting Mistakes in Your Medical Records".[82] It starts by instructing the victim to get copies of his medical records and to manually check them for errors.[83] The advice itself represents a complete detachment from the problem, since, in order to correct medical records, it says to "contact each doctor, clinic, hospital, pharmacy, laboratory, health plan, and location where a thief may have used your information."[84] This suggestion ignores the immense scope of medical identity theft and its dangers. Stolen medical data can be used to receive medical care any place in the country. Furthermore, a single medical visit might involve medical records stored in a variety of areas. For example, a simple patient visit that

[74] *Medical ID Theft/Fraud Information*, *supra* note 1.
[75] *Medical ID Theft/Fraud Information*, *supra* note 1.
[76] *Medical ID Theft/Fraud Information*, *supra* note 1.
[77] *Medical Identity Theft & Medicare Fraud*, OFFICE OF THE INSPECTOR GEN. U.S. DEP'T OF HEALTH & HUMAN SERVS., http://oig.hhs.gov/fraud/medical-id-theft/HHS_OIG_Medical_Identity_Theft _plain_text.pdf (last visited Mar. 17, 2016); *Medical ID Theft/Fraud Information*, *supra* note 1.
[78] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[79] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[80] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[81] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[82] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[83] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[84] *Correcting Mistakes in Your Medical Records*, *supra* note 72.

involves a test and a prescription would leave medical records and debts with three different groups: (1) the doctor, for professional services; (2) a hospital facility, for technical resources utilized for testing; and (3) the pharmacist.

On top of the difficulty of finding out which hospital has the victim's or the thief's medical records under the victim's identity, the page points out that the victim may even have to pay to receive copies of his medical records.[85] Additionally, the FTC notes that a provider might even refuse to give a patient copies of his own medical records, on the grounds that it might violate the privacy rights of the thief who falsely used his identity to receive care.[86] Although patients are entitled to these records, if they encounter a provider who objects, even more hurdles are added.[87] A patient will need to appeal and, if the appeal fails, complain to HHS's Office for Civil Rights.[88]

In addition to a copy of medical records, each patient must also request an "accounting of disclosures" to get a complete picture of how his medical information may have been used.[89] This accounting discloses who received medical records from the provider, what medical information was sent, when and to whom it was sent, and the reason underlying its dispatch, although it may exclude details for routine disclosures.[90] This process could, hopefully, help identify the thief's activities, as the thief would likely catalyze an exchange of the victim's medical records (such as between providers for patient care or referrals, or between the provider and insurer for the filing of claims).[91]

After compiling all these records and asking for any corrections, the victim will need to notify his health insurer and all three national credit-reporting companies.[92] The victim will then need to collect copies of his credit reports, and may even have to place a fraud alert and security freeze on his credit lines.[93]

In addition to all these complicated steps, and not included on the website, is the reality that the medical record amendment process is itself incredibly complicated. The HIPAA Privacy Rule provides patients the right to request an amendment to their records.[94] Providers usually must respond to this request within 60 days, but are not required to change anything within the record.[95] Rather, a provider can deny the request, in which case the patient must go further by requesting that the provider note any disputes with the patient's record.[96]

---

[85] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[86] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[87] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[88] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[89] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[90] *Correcting Mistakes in Your Medical Records*, *supra* note 72.
[91] *Correcting Mistakes in Your Medical Records*, *supra* note 72*; See also* William E. Hopkins, *Medical Identity Theft What It Is and Considerations for the Healthcare Provider*, ABA Health eSOURCE, http://www.americanbar.org/newsletter/publications/aba_health_esource_home/Volume3_06_hopkins.html (last visited Mar. 17, 2016).
[92] *Id.*
[93] *Id.*
[94] *Correction and the Hipaa Privacy Rule*, U.S. DEP'T. OF HEALTH & HUMAN SERVS., OFFICE OF CIVIL RIGHTS 1, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/ healthit/correction.pdf (last visited Nov. 7, 2016).
[95] *Id.*
[96] *Id.*

III. ANALYSIS: INSUFFICIENT REFORM, POTENTIAL SOLUTIONS

The following section reviews the healthcare industry's response to the growing threats posed by medical identity theft, both from criminals targeting insurance payors, providers, and the government, as well as from insufficient protection practices utilized by the above groups. This section also assesses the efficacy of these programs, and notes why they have been insufficient to address the problem. Next, this section discusses two articles that have proposed alternative measures against medical identity theft, and outlines why these measures are lacking.

A. The Industry Responds

In response to the huge problem of medical identity theft, some industry leaders have joined together to research the issue, and to launch the Medical Identity Fraud Alliance (MIFA) in 2013.[97] This group was formed with the overarching goals of better protecting the privacy and security of protected health information (PHI); creating a body of research on the effects of medical identity theft; promoting technologies, policies, and practices to fight medical identity theft; educating stakeholders;[98] and advocating for regulations and policies to fight back against medical identity theft.[99] Those involved in MIFA include insurers, providers, academics, patient groups, and industry groups such as Aetna, Kaiser Permanente, and AARP.[100]

MIFA focuses on several key areas in its recommendations to strengthen the fight against medical identity theft. Among these areas, MIFA examines the lack of transparency and failure in communication between stakeholders early on in the claims process, which is a key obstacle to preventing and remedying medical identity theft.[101] Currently, one of the chief ways that insurers hope to detect medical fraud is through EOB statements.[102] EOBs are sent to patients after benefits are paid out under that patient's insurance coverage.[103] These statements list insurance claims that medical providers and suppliers have filed under patients' insurance coverage.[104] Theoretically, patients read these, then call their insurer to correct any errors, or notify the insurers of any fraudulent charges.[105] In practice, however, many patients may ignore EOBs. Those patients who do read them are frequently only interested in the final amount owed,[106] even though EOBs are not bills, which reinforces patients' confusion. Patients who owe

---

[97] *New Research Reveals Medical Identity Theft Is Up, Affects 1.84 Million U.S. Victims*, MEDICAL IDENTITY FRAUD ALLIANCE (Sept. 12, 2013), http://medidfraud.org/press-release-2013-survey-on-medical-identity-theft/.

[98] Stakeholders, in the context of this Comment, refers to insurers, patients, providers, employers (the most common source of health insurance is an employee benefit), family members, and government.

[99] *About the Medical Identity Fraud Alliance*, MEDICAL IDENTITY FRAUD ALLIANCE, http://medidfraud.org/about/ (last visited Jan. 18, 2015).

[100] *Id.*

[101] *The Growing Threat of Medical Identity Fraud*, *supra* note 4, at 6.

[102] *The Growing Threat of Medical Identity Fraud*, *supra* note 4, at 6.

[103] *Explanation of Benefits*, BLUECROSS BLUESHIELD, http://www.bcbs.com/report-healthcare-fraud/explanation-of-benefits.html (last visited Nov. 16, 2014).

[104] *Id.*

[105] *Id.*

[106] *The Growing Threat of Medical Identity Fraud*, *supra* note 4, at 6.

nothing may be especially unlikely to make a thorough review of the claims listed, as they are not aware of any immediate financial stake.[107] Contrary to credit card companies that have established systems to call and notify a customer immediately after suspicious spending activity is detected, health insurers frequently do not mail an EOB until thirty days after the date on which services were rendered.[108] Therefore, if fraudulent claims are not detected at the point of care, there is often significant lag time between when the fraud occurs, when the victim can begin to seek a remedy, and any repercussions for thieves.[109]

Typically, insurance companies have lagged behind the effectiveness of credit card companies in detecting and preventing fraud. In part, this is because insurance companies tend to pay claims quickly, and then use back-end review and analytics to find fraudulent claims.[110] Insurance companies have had some success in implementing this strategy, although detection has only been post-fraud, rather than utilizing detection to prevent fraud in the first place. An example of one such success involved a fraud scheme from the summer of 2010, in which Yennier Capote Gonzalez created a shell medical corporation in June and filed a number of false claims in July.[111] On August 12, Cigna, an insurance company, mailed Gonzalez's fake medical corporation a check for $38,116.[112] Only afterwards did Cigna report Gonzalez's shell corporation as a suspicious provider, giving notice to a special agent with the HHS.[113] The HHS special agent handling the case eventually coordinated with Gonzalez's bank, and arrested him on August 25, 2010.[114] He was convicted in November 2012.[115] While this is an example of effective detection and ultimately led to conviction of the perpetrator, it is illustrative of reactive, post-fraud handling of medical insurance fraud, rather than the more proactive alternative I propose.

B. Government

Those contemplating the problem of medical identity fraud, who have a surface understanding of HIPAA, would likely think that HIPAA provides patients with some remedies. However, HIPAA is in many ways limited in scope. With regard to medical identity theft, HIPAA can be understood as dealing primarily with two specific areas: (1) protecting patient information from being released, and (2) taking action against those who mishandled patient data.[116] Because this Comment most significantly deals with situations where a breach has already occurred, HIPAA data protection is not relevant to the main argument being advanced. However, HIPAA does highlight the current interplay between state and federal laws governing medical identity theft. HIPAA requires any covered entity that has experienced a patient data breach to report the breach

---

[107] *The Growing Threat of Medical Identity Fraud*, *supra* note 4, at 6.
[108] *The Growing Threat of Medical Identity Fraud*, *supra* note 4, at 6.
[109] *The Growing Threat of Medical Identity Fraud*, *supra* note 4, at 6.
[110] *The Growing Threat of Medical Identity Fraud*, *supra* note 4, at 6.
[111] United States v. Gonzalez, 560 F. APP'X 554 (6th Cir. 2014).
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] *Miami Man Sentenced in Federal Court for Medical Identity Theft Scheme*, UNITED STATES ATT'Y'S OFFICE MIDDLE DIST. OF TENN. (Feb. 19, 2013), http://www.justice.gov/usao/tnm/pressReleases/2013/2-19-13.html.
[116] *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat 1936.

to each individual whose unsecured PHI has been breached.[117] This practice, however, does nothing to address the problem of criminals fraudulently using a patient's personal data at a medical facility. The entity providing care is not necessarily the same one experiencing the data breach, which means HIPAA's protections do not go far enough to be an effective method of preventing medical identity fraud.

The HITECH Act, a 2009 piece of legislation that focused on the digital storage of patient health information, empowers states' attorneys general with the authority to enforce these provisions of HIPAA.[118] They are empowered to bring civil actions on behalf of state residents, and can seek injunctions or statutory damages.[119] However, before they take any actions, they are required by law to provide notice to the HHS, which is statutorily empowered to block actions by state attorneys general.[120] Furthermore, any criminal judgments against HIPAA violators (providers, health systems, and insurers) will be paid to the federal government's Office for Civil Rights to enforce HIPAA compliance.[121]

Most important to understanding HIPAA's deficiencies is accounting for how, in general, when HIPAA and a state law are in conflict, HIPAA will preempt the state law.[122] There are, however, certain instances where HHS may determine that a state law is not preempted by HIPAA.[123] Those circumstances are:

> (1) [t]o prevent fraud and abuse related to the provision or payment of health care; (2) [t]o ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation; (3) [f]or State reporting on health care delivery or costs; or (4) for purposes of serving a compelling need related to public health, safety or welfare.[124]

Furthermore, HIPAA makes it explicit that state standards that are more stringent in their protections for patient information are not preempted.[125] These guidelines and frameworks will be useful in later discussions regarding proposed reforms at both the state and federal levels of government.

Despite its flaws, HIPAA strongly asserts a critical right to preventing medical identity fraud patients' rights to access and amend their medical records.[126] However, these access and amendment portions of HIPAA still have some limits.Providers are only obligated to amend a record that they have generated.[127] Increasingly, medical records are compiled from a variety of sources since hospitals and providers exchange data.[128]

---

[117] Stanley C. Ball, *Ohio's "Aggressive" Attack on Medical Identity* Theft, 24 J.L. & HEALTH 111, 127 (2011).
[118] *Id.* at 128.
[119] *Id.*
[120] *Id.* at 129.
[121] *Id.* at 128.
[122] *Id.* at 129-30.
[123] *Id.* at 130.
[124] *Id.* at 130-31.
[125] *Id.* at 131.
[126] Katherine M. Sullivan, *But Doctor, I Still Have Both Feet! Remedial Problems Faced By Victims of Medical Identity Theft*, 35 AM. J.L. & MED. 647, 660 (2009).
[127] *Id.*
[128] *Id.* at 660–61.

Therefore, if a patient finds a problem in a medical record received by her doctor, she might need to contact a provider she had seen earlier (or, in the case of identity theft, may never have seen) in order to correct the record.[129]

With the widespread adoption of electronic health records, this limit poses an especially dangerous problem. Electronic medical records make it even easier for providers to exchange patient health records.[130] Furthermore, groups such as the American Medical Association have become advocates of health information exchanges (HIEs).[131] HIEs are entities that bring together those who electronically store patient data (usually health systems[132]), and enables them to send information to one another electronically.[133] For the most part, this is good for patients, as it allows health care providers across a wide geographic area to quickly compile a complete patient health history, which could be immensely helpful in delivering care to a patient.[134]

Some HIEs are patient data repositories that collect and store data sent from participating health systems.[135] Other HIEs act more as conduits, where each health system stores the data it collects, but at the request of another system, one institution will send the data for a patient receiving treatment at another institution.[136] Therefore, although electronic health records make it easier for providers to quickly and easily find, store, and create data, in practice the records themselves are a compilation of documentation from a variety of medical care providers.[137] Any incorrect documentation from a medical identity thief that is added to a patient's medical history will be much more easily duplicated and perpetuated. Further, each stakeholder will have a separate set of medical records with the inaccurate information, and the patient will need to contact all health systems that participate in any HIE that transmitted his or her information.[138]

---

[129] *Id.*

[130] Within this Comment, the acronym "HIE" refers exclusively to health information exchanges, explained within. This is not to be confused with the Affordable Care Act's health insurance exchanges, which are also frequently abbreviated with the same acronym. Confusingly, both concepts have recently gained prominence within the healthcare industry.

[131] *Health Information Exchanges*, AM. MED. ASS'N, http://www.ama-assn.org/ama/pub/advocacy/topics/health-information-technology/health-information-exchanges.page (last visited Mar. 12, 2016).

[132] A "health system" is a network of hospitals, clinics, and the related administrative networks.

[133] *Health Information Exchanges*, *supra* note 131. Once an HIE is established, the information exchange occurs entirely electronically. This is in contrast to a group of medical systems that have adopted an electronic health record (EHR), but not joined a network to transmit records. These systems might exchange patient files with one another, but they would not send the information across established computer networks. Rather, the information may be stored on a USB drive or compact disk, and sent through a secure mail or messenger service. HIEs are intended to remove many of the more cumbersome aspects of this sort of exchange of patient information.

[134] *Health Information Exchanges*, *supra* note 131.

[135] *Health Information Exchanges*, *supra* note 131.

[136] *Health Information Exchanges*, *supra* note 131.

[137] *Health Information Exchanges*, *supra* note 131.

[138] *Health Information Exchanges*, *supra* note 131.

C. Potential Reform

1. Stricter Data Protection Requirements

One reform advocate suggests utilizing standards from other data protection laws and applying them to health care.[139] In his article titled *Ohio's "Aggressive" Attack on Medical Identity Theft*, Stanley Ball argues that an Ohio law that has created heightened data security standards should be applied to health care.[140] The law, as written, explicitly does not encompass HIPAA-covered entities.[141] The Ohio statute is designed to protect general personal information, such as name, Social Security number, driver's license numbers, account credit and debit cards numbers, or other information with a code that would permit access to an individual's personal financial accounts.[142]

The law's terms are exceptionally broad, covering "any person [including businesses]" who owns or licenses personal information stored as computerized data.[143] Ohio's statute then requires those covered to notify Ohio residents when a breach in security has been discovered, or if a covered entity knows or reasonably believes that an Ohio resident's personal information was accessed in an unauthorized fashion, and that such access creates a material risk of identity theft or other fraud.[144] The entity must give notification by phone or letter, unless e-mail is the only means of communication.[145] Such notification needs to be given within 45 days after breach discovery.[146]

The Ohio attorney general has sole authority to enforce the Ohio data security law, which includes seeking civil liability, temporary restraining orders, and injunctions.[147] All penalties awarded through enforcement of the law are deposited in a fund solely to be used for the attorney general's consumer protection office.[148]

Ball argues that the Ohio law needs to be broadened to cover healthcare related entities, including those covered by HIPAA.[149] To demonstrate the need, he makes the case that data breaches and lack of security constitute a serious and mostly unchecked problem in healthcare.[150] To support his case, he claims that HIPAA is poorly enforced, and points to statistics that he argues back up that assertion. For instance, he relies on the fact that, between 2003 and 2011, 71% of all HIPAA complaints were dismissed before any formal investigation took place.[151] Furthermore, after investigation 11% of cases were found to have had no violation, and 17% of cases investigated were resolved through agreements with the covered entity or through a voluntary corrective action.[152] Ball also cites a study that says one quarter of respondents to a survey of medical

[139] Ball, *supra* note 117, at 133.
[140] Ball, *supra* note 117, at 133.
[141] Ball, *supra* note 117, at 131.
[142] Ball, *supra* note 117, at 131-32.
[143] Ball, *supra* note 117, at 132.
[144] Ball, *supra* note 117, at 132.
[145] Ball, *supra* note 117, at 132.
[146] Ball, *supra* note 117, at 132.
[147] Ball, *supra* note 117, at 132-33.
[148] Ball, *supra* note 117, at 133.
[149] Ball, *supra* note 117, at 133.
[150] Ball, *supra* note 117, at 133.
[151] Ball, *supra* note 117, at 134.
[152] Ball, *supra* note 117, at 134.

providers indicated that they did not conduct formal risk assessments to detect security gaps for electronically stored patient data.[153]

By HIPAA's own standards, every medical provider should be performing formal risk analyses.[154] Ball's argument assumes that these numbers are obviously indicative of a failure to enforce HIPAA against entities that are careless with patient data.[155] He hopes to broaden the Ohio statute because, since its standards are stricter, it would preempt HIPAA and allow the Ohio state attorney general to bring actions without seeking approval from HHS, thereby streamlining data breach enforcement actions.[156]

Ball's argument misses the point by several measures. First, the percentages he uses (e.g. 71% of HIPAA complaints are dismissed) do not necessarily represent a lackluster enforcement of HIPAA, because they focus on a ratio without sufficient context.[157] In fact, the numbers could represent a pattern of overzealously filing HIPAA complaints without merit. A factor in support of this theory is that HIPAA provides protection against retaliation for whistleblowers.[158] While this is important to protect those who attempt to stop improper PHI handling, it also gives disgruntled employees an incentive to file frivolous complaints.[159] Regarding the other statistics Ball cites, HHS has reasonable goals in agreeing to voluntary corrective actions procedures, and many health organizations may have recognized their mistakes and are attempting to make improvements by agreeing to corrective actions.[160] These statistics should not necessarily be interpreted as reasons to enforce much stricter standards.

The penalties Ball wants enforced against medical providers who are careless with patient data are also misguided. Legal measures addressing medical record breaches should be considered part of a more comprehensive identity theft containment strategy. An appropriate parallel lies in the credit card industry. Because credit card companies recognize that some credit card information will inevitably fall into the wrong hands, they have a strategy that targets stopping suspicious spending behavior at the point of sale.[161] Similarly, insurers could adopt algorithms that look out for unusual patterns of spending and require a second step of identity verification. Just as in the credit card industry, medical identity theft does not always occur because hospitals mishandled PHI. Rather, it often occurs because of the carelessness or laxed security of the insured, a predator who is able to get an individual to reveal his or her insurance number, or an ill-intentioned medical provider who, regardless of whether the HIPAA investigations are stricter, will have access to the patient's billing information.

Despite a short-sighted focus on misleading HIPAA breach investigation numbers, Ball's recommendation that the state law handling patient data protection should adopt

---

[153] Ball, *supra* note 117, at 134.
[154] Ball, *supra* note 117, at 134.
[155] Ball, *supra* note 117, at 134.
[156] Ball, *supra* note 117, at 134.
[157] Ball, *supra* note 117, at 134.
[158] Mary Butler, *HIPAA Whistleblower Protections Promote Information Governance*, JOURNAL OF AHIMA, (Mar. 1, 2014), http://journal.ahima.org/2014/03/01/hipaa-whistleblower-protections-promote-information-governance/.
[159] *Id.*
[160] Ball, *supra* note 117.
[161] Melody Warnick, *7 Reasons Your Credit Card Gets Blocked*, CREDITCARDS.COM (Aug. 6, 2010), http://www.creditcards.com/credit-card-news/7-reasons-credit-card-blocked-tips-for-handling-1282.php.

more consumer remedies for breach of personal medical information is strong.[162] In particular, Ball advocates:

> [giving] citizens some mechanism to recover monetary awards when a business violates the law and the citizen is injured as a result of the violation. The mechanism to recover should be either a civil action brought directly by the citizen against the healthcare provider or a civil action brought by the attorney general entitling a citizen harmed by the statutory violation to a portion of the monetary penalty.[163]

This stands in contrast to HIPAA's limitation on damages, which requires them to be paid out to the OCR, and does very little to right the wrong done to the victim of the breach.[164]

2. Provider Liability

Katherine Sullivan, in a student Note focused on documenting the burdens faced by victims of medical identity theft, briefly mentions her idea of creating a private cause of action against providers as a possible solution for patients who are the victims of medical identity theft.[165] She quickly dismisses the proposal, however, on the grounds that it might cause a flood of litigation.[166] Furthermore, she notes that it does not remedy the problems that victims face in terms of accessing the relevant information, and being able to amend their medical records.[167] She is correct on both of these counts, but the solution of a private right of action still has merit.

If there are a large number of providers who are recklessly sending patients who did not receive any treatment huge medical bills, and being careless with the treatment of patient data, it is more appropriate to hold the provider responsible for correcting the situation, instead of the victim. Furthermore, even though such a reform would not remedy the problems of correcting and amending medical documentation, presumably providers would exercise greater care in treating patients. By increasing the care with which medical professionals handle patient data, and the patients themselves, the number of victims and the volume of medical corrections that need to take place would be reduced.

To deal with the problem of correcting medical record inaccuracies, Sullivan suggests creating a system based on the Fair and Accurate Credit Transactions Act (FACTA).[168] FACTA entitles individuals to periodically receive a free copy of their credit report.[169] Sullivan suggests a similar regulatory framework, but one that would provide patients a free annual report listing all medical services related to an individual's Social Security number.[170] She acknowledges that, at the time she published the article,

---

[162] Ball, *supra* note 117, at 133.
[163] Ball, *supra* note 117, at 142.
[164] 42 U.S.C. § 1320d-5.
[165] Sullivan, *supra* note 126, at 678.
[166] Sullivan, *supra* note 126, at 678.
[167] Sullivan, *supra* note 126, at 678.
[168] Sullivan, *supra* note 126, at 678.
[169] Sullivan, *supra* note 126, at 671.
[170] Sullivan, *supra* note 126, at 679.

due to the lack of pre-existing aggregation of medical claims information (unlike for credit companies), such a tool would be particularly difficult to administratively develop.[171] However, Sullivan was writing in 2009, before the major impact of the HITECH Act in rapidly expanding the adoption of electronic medical records.[172] For this reason, Sullivan's comments are prescient, and with sufficient exposure to the developing health information exchanges, her suggestion presents a useful potential solution.

D. The Burden of De Facto Liability: An Economic Justification for Providers to Bear the Risk

This section outlines the position that the legal and security discussions around health information have focused too narrowly on data-breach prevention, at the cost of finding solutions to minimize the criminal use of stolen personal data in a healthcare setting. Even with reasonable precautions some data is bound to be stolen, and in these cases it is the patients who are responsible for addressing any false medical charges. This de facto liability for patients has disincentivized medical providers from investing in preventative measures, even though they could most easily prevent healthcare fraud.

Many of the most popular justifications for legal liability, such as negligence or the strict liability approach in torts, are rooted in terms of economic efficiency.[173] Although each of these methods has been criticized in a variety of ways, they remain the predominant theoretical justifications for establishing liability.[174] In essence, the question the negligence standard asks is "who can most efficiently reduce the risk of this problem?" while the strict liability system asks, "who benefits from this risk and therefore should bear the cost?"[175]

The credit card industry faces challenges similar to those endured by the medical profession in terms of stolen personal data. To deal with problems arising from stolen credit cards or personal data, credit card companies have developed processes to prevent and detect the unauthorized use of personal credit card information.[176] To avoid negative financial impacts on credit card holders, Visa uses sophisticated credit card monitoring tools, such as complex algorithms to detect and stop fraudulent transactions at the point of sale.[177] Because credit card companies bear the financial risk for unauthorized use of a credit card, they have developed this multifaceted approach that encourages not only data protection, but also prevention of information theft at the point-of-use level.[178]

In the medical industry, patients are essentially the only party that cannot do anything to prevent the use of stolen data. There are roughly three parties to any healthcare transaction: patients, providers, and insurers. After his or her insurance information is stolen, any individual patient is unlikely to have any contact with the thief.

---

[171] Sullivan, *supra* note 126, at 679.
[172] Sullivan, *supra* note 126, at 679.
[173] Jason S. Johnston, *Punitive Liability: A New Paradigm of Efficiency in Tort Law*, 87 COLUM. L. REV. 1385, 1385 (1987).
[174] *Id.*
[175] *Id.* at 1393.
[176] *See, e.g.*, *CPS/Card Not Present*, VISA, https://usa.visa.com/content/dam/VCOM/download/merchants/VBS-07-APR-14-CPS-card-not-present.pdf (last visited Mar. 18, 2016).
[177] *See, e.g.*, Description of Security Program, VISA, https://usa.visa.com/support/consumer/security.html (last visited Mar. 18, 2016).
[178] *See, e.g.*, *id.*

However, by the very nature of the crime, the thief will certainly be in contact with providers, who will subsequently be in contact with insurers. Thus, saddling patients with responsibility for determining what happened, and with bills for care they did not receive makes the least sense. As such, specific statutes are necessary to ensure that patients receive the most protection in the unfortunate event of medical identity theft.

While Ball's proposal to impose civil liability on hospitals would be a step in the right direction in terms of deterring medical identity theft, his proposal is more blunt than necessary to be an effective solution to the problem.[179] The main drawback to his proposal is that it does not reach the full spectrum of the problem of medical identity theft. Rather, it seeks to minimize damage from hospital breaches, and operates under the assumption that by giving citizens a significant remedy against hospitals, hospitals will begin exercising more care with patient data, thereby stopping medical identity theft. The gap in the logic lies in the belief that stricter, more careful handling of patient data storage processes will lead directly to stopping medical identity theft. For this to be the case, Ball would need to establish that the majority of medical identity fraud occurs because providers are careless with patient information. Even if we accept Ball's premise that large numbers of providers are careless or negligent in their handling of patient information, it does not follow that this is the source of information for those perpetrating medical identity theft. As outlined above, criminals access information critical to patient identity in a variety of ways.

Every day millions of Americans are threatened by new, unforeseeable risks, no matter how reasonable their efforts to protect their personal data. An example of this danger is the Heartbleed Bug problem.[180] Revealed in early 2014, this was a software bug in commonly used encryption technology that allowed others to easily learn what passwords people used for their different accounts.[181] Considering the amount of personal data stored in different personal online accounts, it is not unreasonable that a criminal could have used this bug to gain personal information, such as a Social Security number, that would allow him or her to receive treatment at a hospital, or (through online patient portals) schedule appointments with providers and then present to receive care. Even citizens who took every reasonable caution were vulnerable to this threat. Although Ball provides a strong overview of the problem of medical identity theft,[182] he does not explain how his proposal would fight back against these types of problems.

Given the numerous ways to access vulnerable patient information, any approach to the medical identity fraud problem needs to tackle the issue from multiple angles. First, the legal regime should have, as Ball outlined, a proactive deterrent against mishandling of patient data in order to prevent breaches in the first place. Second, any solution to the medical identity theft problem also needs to provide additional preventative measures, such as requiring hospitals to ensure that patients who show up to clinics are indeed who they claim to be. Finally, the medical identity theft problem also needs reforms that allow patients to more easily correct their medical records, and must provide legal recourse against providers who bill patients for services the patients did not receive.

---

[179] *See* Ball, *supra* note 117.
[180] Bruce Schneier, *Heartbleed*, SCHNEIER ON SECURITY, https://www.schneier.com/blog/archives/2014/04/heartbleed.html (last visited Mar. 18, 2016).
[181] THE HEARTBLEED BUG, http://heartbleed.com/ (last visited NOV. 26, 2016).
[182] Ball, *supra* note 117, at 117–22.

A solution to this problem is shifting the de facto liability for medical identity theft from the victims to providers. This shift in responsibility will encourage providers to adopt more stringent security measures, such as better patient identification practices. Furthermore, because of recent advances in technology, these measures can be adopted at a reasonable cost, and will be especially effective if combined with interoperability initiatives, such as HIEs.

1. Data Protection Statutes

Ball also offered a proposal for more stringent data protection measures that are a strong step in the right direction of expecting hospitals to exercise greater care.[183] The specific details will not be covered here, but any final proposal should adopt the principles of greater patient autonomy in their ability to bring charges. 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.

2. Illicit Data Use Prevention

The proposals outlined in this Comment are much stronger and better tailored than both current law and existing proposals in the area of preventing the inappropriate use of a patient's information. In particular, this Comment proposes a stronger set of requirements regarding verification of patient identity within hospitals. Although the process of identification could be costly, there are more tools available to hospitals to verify patient identity than ever before, some of which have a very low cost.

During the patient registration process, providers will frequently ask a patient only for his name and date of birth to verify his identity. Hospitals could take a number of additional steps that would further verify a patient's identity. These measures include photographs, biometric data, and stronger patient background documentation.[184] For example, many hospitals have electronic health records that could store photos taken of patients when they first present for registration.[185] This process would not work for hospitals where the true patient had not been before, but if a thief tried to use the same hospital as the victim, he or she might be thwarted. Although using biometric data (such as fingerprints or eye scans) for patient care might currently be cumbersome, the technology used for these processes is improving every day.[186] While hospitals may not

[183] Ball, *supra* note 117, at 133.
[184] Although biometrics are now being used primarily for hospital employees and physicians, it is easy to imagine the additional step of extending biometric identification to the patient. *See, e.g.*, Howard Anderson, *Biometrics' Role in EHR Rollout*, HEALTHCARE INFO SECURITY (Dec. 2, 2011), http://www.healthcareinfosecurity.com/biometrics-role-in-ehr-rollout-a-4298.
[185] *E.g.*, *Patient Photos for Medical Record*, PINNACLE HEALTH, available at http://www.pinnaclehealth.org/services-and-resources/preparing/patient-photos-for-medical-record/ (last visited Nov. 13, 2016).
[186] *Id.*

yet have a strong incentive to adopt such technology, with a burden of liability for failing to prevent medical identity theft, they might begin to do so.

Although ultimate responsibility for medical identity theft should obviously lie with the thief, the perpetrators will be difficult to track down. Furthermore, because medical identity theft may frequently be crime of desperation, even if the true criminal is tracked down, he or she could be insolvent and therefore judgment-proof. Despite having done nothing wrong, patients are de facto liable for the crimes of others, and for the lasting effects of medical identity theft. The difficult, painful, back-and-forth processes involved in contesting charges means that many patients might decide to simply pay the false bills they receive, then change insurance information to stop any further thefts going forward.

As discussed earlier, of the non-criminal parties, the patient is the least reasonable person upon whom to place the cost of medical identity theft. The patient has the least ability to prevent the illicit use of his or her insurance information. Hospitals, on the other hand, have a number of additional steps they could take to improve patient identity verification. Hospitals commonly take simple steps, such as taking a scan of a patient's driver's license to store. However, whether they do this on each visit, or only an initial visit to the hospital, is less standardized.

Other critics might suggest that, rather than place liability at the hand of the provider, liability should be placed on the insurer. While hospitals have deeper pockets than patients, insurance companies are likely to have even deeper pockets. However, insurers would still need to rely on the hospitals to prevent illicit use of patient information. At the end of the day, an insurer has no control over whether a patient receives care. Behavioral profiles as are used in the credit card industry, do not make as much sense in healthcare, because treatment is often needed at unusual times, not at a steady, trackable pace.[187] For these reasons, providers remain the party that should bear the burden of preventing fraudulent treatment. In particular, liability should be applied to hospitals because they have the lowest cost of prevention after a patient's identity has been stolen. Whereas a patient would have to follow the onerous process described earlier, a hospital would simply be asking additional questions before services were delivered under fraudulent pretenses.

3. Remedies For Patients Against Hospitals

The remedies available to patients who fall victim to false bills from medical identity theft ought to include all legal fees incurred by the victims and any lost wages due to missing work to deal with the repercussions of medical identity theft. Currently, the process of fighting medical identity theft can cost patients tens of thousands of dollars in medical and legal bills, in addition to huge time investment trying to resolve the issue. There is currently no way for patients to avoid these costs, and hospitals have no incentive to change their protocols, continuing to send bills to patients, fraudulent or otherwise.

[187] There are some cases where there is an obvious discrepancy between a patient's condition and his (fraudulent) insurance claims (e.g. foot surgery on a patient with no legs), however, these are a small percentage of medical identity theft cases. Although insurance companies do monitor this to some extent, the efficacy is much more limited than the analogous monitoring used in the credit card industry.

Some might say shifting the burden for inappropriate billing would place too heavy of a responsibility upon small, independent practitioners. Despite trending towards larger healthcare organizations, small, independent medical practices remain key features of the American healthcare landscape.[188] While the need to refrain from unfairly burdening independent providers does create a problem, it does not negate the need for active patient protection. At the end of the day, even if the provider must pay a bit more to verify patient identity, it is a more effective use of funds than spending money to correct the effects of medical identity theft after it has occurred. Furthermore, visits to small, independent medical clinics are, by their nature, less likely to be highly expensive, since even independent medical practitioners who perform expensive procedures typically need to partner with a larger healthcare organization to do so.[189]

4. Other Avenues for Patient Protection

Beyond remedies involving the courts, other methods exist by which the government could provide significant protections for patients. One key area is through the widespread adoption and standardization of HIEs, alongside regulation for electronic medical record interoperability. One of the key obstacles to hospitals forming an HIE lies in the different ways that patient data is stored across hospitals.[190] There are a large number of different electronic medical records systems on the market, and each stores data in different ways in terms of file structure, format, and language.[191]

An analogy to various paper storage systems illustrates the problems with combining files from different healthcare providers. Hospital A, for example, stores all its patient records alphabetically. Hospital A records patient encounter information on a form that includes sections such as "Date of Visit," "Symptoms," "Diagnosis," "Current Medications," and "Recommended Treatment." After each section there is a blank space where the doctor can write in the information as he sees fit, and the doctors all write in English. Hospital B, however, stores all its patient records chronologically, rather than alphabetically. It has paper forms that include all the same sections as Hospital A's forms, except that they are written in Portuguese. Furthermore, rather than having blank space after each section, Hospital B's form has a series of checklists. For example, it has the most common symptoms written out with a box to check next to each: "stomach aches," "fever," "cough," "headaches," "chest pain," and so on. Instead of a blank space after the date, it has fields labeled "(MM/DD/YYYY)".

---

[188] Larry Myler, *The Private Medical Practice is Not Dead*, FORBES (Jun 16, 2015), http://www.forbes.com/sites/larrymyler/2015/06/16/the-private-medical-practice-is-not-dead-yet/#757ea3b52e40; *See also* David Squires and David Blumenthal, *Do Small Physician Practices Have a Future?*, THE COMMONWEALTH FUND (May 26, 2016), http://www.commonwealthfund.org/publications/blog/2016/may/do-small-physician-practices-have-a-future.

[189] Avik Roy, *Hospital Monopolies: the Biggest Driver of Health Costs That Nobody Talks About*, FORBES (Aug. 22, 2011), http://www.forbes.com/sites/theapothecary/2011/08/22/hospital-monopolies-the-biggest-driver-of-health-costs-that-nobody-talks-about/#7bafac211f5b.

[190] Philip Aspden et al., *Patient Safety: Achieving a New Standard for Care* (2004), at 127–28, https://www.nap.edu/read/10863/chapter/7 (last visited Nov. 13, 2016).

[191] *See* Michelle McNickle, *8 Common Questions About HL7*, HEALTHCAREIT NEWS (Apr. 25, 2012), http://www.healthcareitnews.com/news/8-common-questions-about-hl7 (noting the need for a common communication structure between EHRs).

The discrepancies between these two systems demonstrate how difficult it would be to compile separate records into one cohesive source of information for patients. While it is certainly possible to take the information from one of the records and translate it into a format that would fit into the other filing system's format, it is a time- and work-intensive process. Likewise, different electronic medical records need to have information converted into compatible formats in order to communicate with one another.[192] Data interfaces can be set up to facilitate the communication between different systems. Because essentially the same conversions will happen over and over again throughout the sending of thousands of records, these interfaces, once set up, are much more efficient than a manual translation of records would be. However, interfaces do require some continual maintenance, since updates to either storage system will likely require updates to the interface, and since interfaces can use large amounts of bandwidth and computer processing power.[193]

Due to of the various problems that storing information in different formats poses, the American Medical Association has called for the standardization of electronic medical record formats, particularly with respect to user interfaces.[194] Standardized interfaces would engender more standardized data storage formats, thus, increasing the ease of communication. Better standardization also means increased ability to make corrections to patient medical records, since the specific fields and records containing incorrect patient information could be much more readily identified, tracked, and updated.

Critics of standardization of EHRs argue that it will stifle innovation and experimentation that is crucial to the development of more effective technology.[195] One solution to this dilemma could be to create standardization for HIEs.[196] HIEs could be required to store their information in a format that allows them to communicate easily with other HIEs, while accepting and interpreting various EHR formats.[197] This helps minimize any potential stifling of innovation, because it only requires a small area of technology to operate under explicit government guidelines, but allows EHR functionality more broadly to change with new innovations.

In terms of the financial impact of these changes, initial studies on electronic health records indicated an estimated $81 billion in annual savings for overall healthcare

---

[192] *Id.*

[193] *Hosted v. On-premise EHRs*, BEI NETWORKS (Aug. 2011), http://www.beinetworks.com/Whitepaper_HostedvsOnPremiseEHR.php.

[194] *AMA Calls for EMR Standardization to Ease Physician Use*, FIERCE HEALTHCARE (June 23, 2011), http://www.fiercehealthcare.com/ehr/ama-calls-for-emr-standardization-to-ease-physician-use.

[195] Janice Simmons, *AMA Report: Standardizing EMRs Would 'Stifle Innovation'*, FIERCEEMR (May 12, 2011), http://www.fierceemr.com/story/ama-report-standardizing-emrs-would-stifle-innovation/2011-05-12.

[196] Jan Walker, et. al., *The Value of Health Care Information Exchange and Interoperability*, HEALTH AFFAIRS, 16 (Jan. 19, 2005), http://content.healthaffairs.org/content/early/2005/01/19/hlthaff.w5.10.full.pdf+html?sid=cc01561b-8e92-4f15-81a9-a4621bbce89d.

[197] *Id.* There are a large number of HIEs each separately attempting to assemble their own networks between hospitals. Some are for-profit, other non-profit, but each can have different standards for their data.

expenditures from investments in healthcare IT.[198] Despite these projections, overall annual healthcare expenditures actually grew by $800 billion.[199] Critics of the initial study predicting $81 billion in savings argued that the study failed to account for the costs of poorly designed software and resistance from clinicians to adopting new systems.[200] Adding the interoperability standards discussed above could help both EHRs and HIEs reach their true savings potential by further incentivizing utilizing the most updated technology.[201] Given the overall benefits of standardization, opposition to such progress would become penny-wise, but pound-foolish.

Additionally, the federal government should mandate that HIEs include a system that allows patients to request a compilation of their records from hospitals that are participating in any particular HIE. This ability could be combined with a process that allows patients to correct their records through the HIE, rather than contacting each hospital directly. Such a policy could severely reduce the cost to patients of having to proactively search for any hospital or clinic at which a criminal could have possibly used the victim's information.

Together, these last two proposals for interoperability and patient access to data could lead to the creation of effective electronic personal health records (PHRs), without the intrusive, administrative-heavy approach of creating national patient identifiers, which some have advocated.[202] PHRs are personal collections of health information that are owned and controlled by the patient, while EHRs are owned and controlled by a health provider, and usually only include information created or directly sent to the provider.[203] This is a significant distinction because it gives patients a way to create a more comprehensive health record.[204] One of the obstacles to adoption of PHRs by consumers is the large amount of time it takes to build—many require patients to manually enter their own information.[205] Many proposals for improving patient care at a lower cost focus on remote patient monitoring through smartphones and other devices, and blending these disparate sources of information into one record would streamline the entire process.[206] These proposals could be effectively and quickly adopted once the appropriate legal incentives were in place to protect patients from de facto liability.

---

[198] Arthur L. Kellerman & Spencer S. Jones, *What It Will Take To Achieve The As-Yet-Unfulfilled Promises Of Health Information Technology*, 32 HEALTH AFFAIRS 63, 63 (Jan. 2013), http://content.healthaffairs.org/content/32/1/63.full.pdf+html.

[199] *Id.*

[200] *Id.*

[201] *Id.* at 64.

[202] Derek Ritz, *OPINION: It's Time for a National Patient Identifier*, HEALTH INFO. MGMT. SYS. SOC'Y (July 11, 2013), http://www.himss.org/News/NewsDetail.aspx?ItemNumber=21464.

[203] *EHR/PHR Basics*, NIH MEDLINEPLUS (Summer 2009), http://www.nlm.nih.gov/medlineplus/magazine/issues/summer09/articles/summer09pg17.html.

[204] *Personal Health Records and the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., OFFICE OF CIVIL RIGHTS, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding /special/healthit/phrs.pdf (last visited Mar. 10, 2016).

[205] Nicole Lewis, *Consumers Slow to Adopt Electronic Personal Health Records*, INFO. WEEK (Apr. 4, 2011), http://www.informationweek.com/healthcare/electronic-health-records/consumers-slow-to-adopt-electronic-personal-health-records/d/d-id/1097077?.

[206] Pamela Lewis Dolan, *Smartphones, Other Devices May Boost Use of Personal Health Records*, AM. MED. NEWS (Sept. 21, 2010), http://www.amednews.com/article/20100921/business/309219997/8/.

IV. CONCLUSION

Medical identity theft is a large and growing problem for patients in America's health care system. The problem demonstrates the need for all people to closely guard their personal information, because the consequences for failing to do so can be dire and unexpected. However, even with proactive data protection, so much personal information lies in the hands of others that even the most careful person could have his or her identity stolen.

Regulatory authorities need to take extreme care to ensure that hospitals are not the source of these breaches. Further, medical providers should bear the burden for ensuring that they do not impose the harm of medical identity theft on patients through the providers' failure to adequately verify the identity of those receiving care. For those providers that do give care to those using false identities, they should bear the burden of ensuring correction of patient records. New developments in the health information technology landscape should, hopefully, make this an easier burden for hospitals to bear.