THE RIGHT TO BE FORGOTTEN: APPLYING EUROPEAN PRIVACY LAW TO AMERICAN ELECTRONIC HEALTH RECORDS

Jordan D. Brougher*

I. INTRODUCTION

Imagine Jane Doe wakes up one morning and turns on the local news to find her health insurance provider, XYZ Insurance, is the victim of a cyberattack. A few days later she receives a letter informing her of the breach and that her data has been compromised. XYZ promises to provide identity theft protection for the next year. Jane places the letter in a folder containing three similar letters from other

* J.D. Candidate, 2016, Indiana University Robert H. McKinney School of Law; B.S., 2011, Indiana University. I would like to thank my wife, Kourtney, and the rest of my family for their continued love and support.

http://dx.doi.org/10.18060/3911.0025

corporations which have suffered recent breaches. She feels helpless as cybercriminals now have access to her private medical information.

With the 2014 and 2015 data breaches at major corporations like Sony Pictures, Community Health Services, Target, and most recently Anthem, our individually identifiable medical information becomes increasingly at risk. Large corporations like Sony Pictures and Anthem store their employees' personal information through a system of electronic records.[1] The Sony cyberattack occurred during the build-up to the release of a comedy film depicting the attempted assassination of the North Korean Supreme leader, Kim Jong-un.[2] The attack illustrates a great cause of concern for employees across the United States. Employers hold valuable employee information such as Social Security numbers, salaries, performance reviews, and personal medical information.[3]

Additionally in February 2015, Anthem, one of the nation's largest health insurers, headquartered in Indianapolis, reported a breach that could affect up to 80 million customers and employees.[4] Anthem CEO, Joseph R. Swedish, believes the hack to be a "very sophisticated external cyberattack" with the cybercriminals accessing personal information like Social Security numbers and birthdates.[5] However, the Federal Bureau of Investigation is looking into whether health information was stolen or not.[6]

---

[1] Cyberattacks are performed by groups targeting employee and customer stored information such as Social Security numbers, credit card information, and health information within the targeted companies' computer systems. Andrea Peterson, *Lawsuits against Sony Pictures Could Test Employer Responsibility for Data Breaches*, WASH. POST (Dec. 19, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/19/lawsuits-against-sony-pictures-could-test-employer-responsibility-for-data-breaches/ [http://perma.cc/U36E-U8BW].

[2] *See id.*

[3] *Id.*

[4] Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, NY TIMES (Feb. 5, 2015), http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html?_r=0 [http://perma.cc/7V4M-C739].

[5] *Id.*

[6] *Id.*

The most troubling part of the cyberattacks is the evidence showing that companies cut corners on data security to save money.[7] However, corporations that choose to cut corners ultimately pay a steeper price in the end, as do their employees. By failing to secure protected health information, data breaches can result in hefty fines from the Department of Health and Human Services (HHS) and monetary damages in the range of several million dollars.[8]

A major difference exists between the Sony attack and the Anthem attack. While Sony is a leader in the entertainment industry, Anthem is a leader within the health care industry. Yet, the Sony cyberattack allowed the cybercriminals to gain access to employee medical records including information on surgeries, therapies, and medical diagnoses such as cancer, kidney failure, and premature births.[9] Even though, cybercriminals mostly use the stolen information for identity theft purposes, there is a potential to use the information in the service of other crimes such as insurance and prescription fraud.[10] Meanwhile Sony will incur liability for the breach as

---

[7] Peterson, *supra* note 1.

[8] Annually, data breaches cost the health care industry around $5.6 billion, and as more health care providers go to the electronic health record "cloud" this number is expected to continue to increase. Jason Millman, *Health Care Data Breaches Have Hit 30M Patients and Counting*, WASH. POST (Aug. 19, 2014), http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/ [http://perma.cc/B89L-7X8B] (citing Chris Burt, *Data Breaches Cost Healthcare Firms $5.6 Billion Annually: Ponemon Institute*, WHIR (Mar. 19, 2014), http://www.thewhir.com/web-hosting-news/data-breaches-cost-healthhealthhealth care-firms-5-6-billion-annuallay-ponemon-institute [http://perma.cc/92VJ-2C4U].

[9] Peterson, *supra* note 1.

[10] Pragati Verma, *Why Medical Data is Vulnerable—And Valuable—To Cybercriminals*, FORBES (Mar. 12, 2015, 4:59 PM), http://www.forbes.com/sites/teradata/2015/03/12/why-medical-data-is-vulnerable-and-valuable-to-cybercriminals/ [http://perma.cc/UM46-73LM]; *see also* Caroline Humer & Jim Finkle, *Your Medical Record is Worth More to Hackers Than Your Credit Card*, REUTERS (Sept. 24, 2014), http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 [http://perma.cc/H9YG-MXF8] ("Fraudsters use [health] data to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number

it is required by California law to keep medical information separate from other employee information in a different security system.[11]

The Sony and Anthem cyberattacks show the rapidly increasing inability of the United States' Health Information Portability and Accountability Act (HIPAA) and subsequent state law to properly motivate companies to protect patient data. The Act fails to provide a private right of action for individuals, like the Sony employees, who, as a result of their employers' inability to protect the information, have theirs stolen.[12] Congress must both strengthen HIPAA to better protect individual patient data and provide individuals with a private right of action.

This Note will discuss the need to strengthen health information data protections under HIPAA. In comparing the United States and European Union ("EU") privacy law, the Note will address the benefits and shortcomings of each approach. Furthermore, the Note will look to European law and its "right to be forgotten." Then, the Note will apply the principles of the EU right to be forgotten to American health records and health information. Finally, the Note will address issues pertaining to the right to be forgotten and the reasons why Americans do should want the right added to the constitutionally recognized right of privacy.

A. The Issue: HIPPA's Inability to Protect Patient Health Records

Health care data has increasingly become the target of data breaches accounting for nearly "43 percent of [all] major data breaches reported in 2013."[13] While some breaches are the result of employee negligence, most are done with

---

with a false provider number and file made-up claims with insurers . . . .").

[11] Peterson, *supra* note 1.

[12] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in various sections of 42 U.S.C.).

[13] Millman, *supra* note 8.

malicious intent.[14] The trend is disturbing, because there are multiple avenues for a breach to occur, and it indicates a lack of security. Under the 2009 HIPAA Breach Notification Rule, HIPAA "covered entities" and their "business associates" must follow federal reporting requirements.[15] The requirements necessitate that covered entities notify affected individuals,[16] the Secretary of the Department of Health and Human Services (HHS),[17] and, if more than 500 residents of a State are affected, the media outlets serving the State.[18] HHS has tracked 944 major breach reports affecting nearly 30 million people.[19] Steve Weisman, a law professor and contributor to USA Today, predicts that the source of most data breaches in 2015 will target the health care industry.[20] To explain his prediction, Weisman focuses on the large amount of information being shared by entities and the lack of proper security.[21] Weisman's prediction should frighten the health care industry and the country.

Patients have few means to persuade health care corporations to adequately protect their information. Patients may "shop" around for corporations that will better protect their data. However, patients subject to a health maintenance organization ("HMO") plan provided by an employer will not have this luxury. Under an HMO plan, a patient may only go to doctors, other health care providers,

---

[14] *See* Dan Munro, *Cyber Attack Nets 4.5 Million Records From Large Hospital System*, FORBES (Aug. 18, 2014, 9:01 AM), http://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/ [http://perma.cc/ 8QY2-JYK2] ("83.2% of 2013 of patient records breached in 2013 resulted from theft").

[15] HIPAA Breach Notification Rule, 45 CFR § 164.404- (2016).

[16] 45 CFR § 164.404 (2016).

[17] 45 CFR § 164.408 (2016).

[18] 45 CFR § 164.406 (2016).

[19] Millman, *supra* note 8.

[20] Anthem's data breach provides concrete evidence that Professor Weisman's prediction holds weight and members of the health care industry must strengthen their cyber-security. Steve Weisman, *Cyber Predictions for 2015*, USA TODAY (Dec. 20, 2014), http://www.usatoday.com/story/money/personalfinance/2014/12/20/cyber-hack-data-breach/20601043/ [http://perma.cc/J33H-QJJ2].

[21] *Id.*

and hospitals on the plan's list.[22] Since the late 1990s, managed care has dominated the health care marketplace with more than 70 million Americans enrolled in HMOs and 90 million enrolled in PPOs (preferred provider organizations).[23] While HMO enrollment numbers have been in decline, managed care is still a dominant form in the health care market place[24] and limits the patient's ability to hold the company accountable in protecting their data. In a recent interview on Sound Medicine Radio, Titus Schleyer, Director of Regenstrief Center for Biomedical Informatics in Indianapolis, stated "as a patient you are so removed from control over your information that you really can't do anything."[25] Schleyer goes on to argue that stolen health information is of little use to cybercriminals, because the information does not provide as good of a benefit as stolen data like Social Security numbers and birthdates.[26] Schleyer's comments illustrate the miscommunication between patients and providers. Patients may believe their information is staying within their providers' systems when in reality it is being sent to the health storage cloud or to another corporation for storage.[27] This reality should be reflected in an informed consent form, (even if patients will

---

[22] *Health Maintenance Organization (HMO) Plan*, MEDICARE.GOV, http://www.medicare.gov/sign-up-change-plans/medicare-health-plans/medicare-advantage-plans/hmo-plans.html [http://perma.cc/AX8E-CHQH] (last visited Feb. 7, 2016).

[23] *Managed Care, Market Reports and the States*, NCSL, http://www.ncsl.org/research/health/managed-care-and-the-states.aspx [http://perma.cc/H4R3-EDCS] (updated June 2013).

[24] *Id.*

[25] *In the Era of Cloud Health Data, Safety is Not Guaranteed*, SOUND MEDICINE RADIO (Feb. 27, 2015), http://soundmedicine.org/post/era-cloud-health-data-safety-not-guaranteed#.VP8DJBneQ4s.email [http://perma.cc/7RSH-F6ZP] (explaining once providers place patient information in EHRs with another corporation or in the health storage cloud, the providers are not even sure where the information is at any given time).

[26] *Id.* Schleyer's argument contradicts others regarding the use of health information for criminal purposes. *See* Verma, *supra* note 10.

[27] *See* Erin Gilmer, *Privacy and Security of Patient Date in the Cloud*, (April 16, 2013), https://www.ibm.com/developerworks/cloud/library/cl-hipaa/ [https://perma.cc/L4AS-SCHT].

never read the form), that is signed upon the collection of their information.

Health care industry expenditures made up roughly 17.1% of the United States' gross domestic product ("GDP") from 2010-2015.[28] The World Health Organization database calculates the percentage based on expenses both public and private including preventative and curative health services, family planning activities, nutrition activities, and emergency aid.[29] To contrast the United States with other economic leading countries, the United Kingdom's expenditures represent only 9.1% of its GDP, and France's expenditures represent 11.5% of its GDP from 2010-2015.[30] The United States must find a way to lower the proportion of health care spending within its GDP.

Furthermore, corporations in the United States will continue to spend in the billions to rectify patient record security breaches.[31] In August 2014, Community Health Services announced the second largest breach in U.S. history affecting more than 4.5 million patients and potentially costing above $77 million in fines and remedies.[32] Community Health Services, located in Tennessee and serving twenty-nine other states, believes "the attacker was an 'Advanced Persistent Threat' group originating from China" targeting Community Health Services systems with "highly sophisticated" technology.[33]

One of the largest fraudulent uses for stolen health records is medical insurance fraud. The most common method by which criminals fraudulently obtain patient

---

[28] WHO Global Health Expenditure Database, *Health Expenditure, Total (% of GDP)*, WORLD BANK, http://data.worldbank.org/indicator/SH.XPD.TOTL.ZS/countries/1W?display=default [http://perma.cc/6XG7-KUTP] (last visited Feb. 7, 2016).

[29] *Id.*

[30] *Id.*

[31] According to benchmark research performed by the Ponemon Institute on the cost of data breaches, each compromised record costs the company an average of $201. Taking the Anthem data breach with nearly 80 million records compromised, it would result in a cost of $16 billion. *See* PONEMON INST. LLC, 2014 COST OF DATA BREACH STUDY: UNITED STATES 1 (2014), *available at* http://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03017usen/SEL03017USEN.PDF [http://perma.cc/RA6K-R4TU].

[32] Munro, *supra* note 14.

[33] *Id.*

information is by "inducing medical personnel with access to patient insurance information to copy the information and provide it to those involved in fraud schemes"[34] and "[p]urchasing the information from others involved in fraud . . . marketers of stolen patient and physician billing information."[35] "Estimates of fraudulent billings to health care programs, both public and private, are estimated between 3 and 10 percent of total health care expenditures."[36] Medicare and Medicaid have been subject to losses in the billions from healthcare fraud.[37] This amount includes provider and patient fraud outside the scope of stolen health care records.[38] The government's health care fraud prevention and enforcement recovered $4.3 billion in taxpayer dollars as part of the Obama administration's attempts to eliminate health care fraud and reduce health care costs.[39] With tax-funded programs facing fraud, taxpayers have even more incentive to protect their information in order to potentially lower the taxes necessary to fund these programs. While fraud can come from many sources, not all can be attributed to medical identity theft. For example, Stark and Anti-Kickback violations are

---

[34] White-Collar Crime, *Health Care Fraud Overview*, THE FBI, http://www.fbi.gov/about-us/investigate/white_collar/health-care-fraud/health-care-overview [http://perma.cc/B96W-PMD8] (last visited Feb. 7, 2016).

[35] *Id.*

[36] *See* FED. BUREAU OF INVESTIGATION, FINANCIAL CRIMES REPORT TO THE PUBLIC 2007, at 9 (2007), *available at* https://www.fbi.gov/stats-services/publications/fcs_report2007 [http://perma.cc/FU5J-BBEQ] (explaining "[e]stimates of fraudulent billings to health care programs, both public and private, are estimated between 3 and 10 percent of total health care expenditures.").

[37] *By the Numbers: Fraud Statistics*, Coalition Against Insurance Fraud, Healthcare, (last visited May 20, 2016) http://www.insurancefraud.org/statistics.htm#.V0HcXPkrLIU. [https://perma.cc/9ACQ-X9GF].

[38] *Id.*

[39] U.S. Dep't of Justice, *Departments of Justice and Health and Human Services Announce Record-Breaking Recoveries Resulting from Joint Efforts to Combat Health Care Fraud*, (Feb. 26, 2014), http://www.justice.gov/opa/pr/departments-justice-and-health-and-human-services-announce-record-breaking-recoveries-0 [http://perma.cc/GJ5P-EKL8].

frequently found against health care providers claiming more money than they are entitled to.[40]

As the Patient Protection and Affordable Care Act ("ACA") became law, the United States started to focus on the soaring costs of the health care industry.[41] The ACA is an attempt to provide affordable coverage to Americans by creating new tax credits and new marketplaces where competition will lead to better prices and better results.[42] In the Ponemon Institute's "Benchmark Study on Patient Privacy & Data Security", two-thirds of health care organizations feel the new law increases the risk of data breaches.[43] Beginning in 2012, ACA section 1561 called for the standardization of billing and the adoption and implementation of an electronic exchange of health records.[44] The ACA increases the concerns over the "exchange of patient information between [healthcare] providers and government organizations."[45] The call for increased electronic health records ("EHR") combined with organizations' poor security practices place patient information at risk.[46] Organizations must take more responsibility under the ACA to protect patient information. For example, data encryption should be mandatory for any company device that leaves the office. The ACA's effects on patient information data breaches have yet to materialize, but providers, patients, and the government must do more to protect patient information.

---

[40] U.S. Dep't of Health and Human Servs, *Medicare Fraud & Abuse*, (Aug. 2014), https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/Fraud_and_Abuse.pdf. [https://perma.cc/RX6U-7V6Y].

[41] *Health Care that Works for Americans*, WHITEHOUSE.GOV, http://www.whitehouse.gov/healthreform/healthhealthhealthcare-overview [http://perma.cc/W4RP-HCA6] (last visited Feb. 7, 2016).

[42] *Id.*

[43] Jeffrey Bendix, *Healthcare Data Breaches Decline, but ACA Could Be Increasing Risks*, MED. ECON. (May 15, 2014), http://medicaleconomics.modernmedicine.com/medical-economics/content/tags/affordable-care-act/healthcare-data-breaches-decline-aca-could-be-inc?page=full [http://perma.cc/8PHJ-FWBW].

[44] 42 U.S.C. § 300jj-51 (2015).

[45] Bendix, *supra* note 43.

[46] *Id.*

B. European Issues With Health Record Data Breaches

The United States is not alone in experiencing patient information data breaches. In a 2014 study, by the Central European University's Centre for Media, Data and Society (CMDS) reported that shows the European Union's twenty-eight countries of the EU have suffered 229 known data breaches "covering 227 million personal records."[47] However, the European Union addresses individual privacy rights much differently than the United States does.

The EU acknowledges privacy as a fundamental right.[48] European institutions have a difficult time defining what the right entails and instead take "a piecemeal approach to defining private life, rather than providing a general or exhaustive definition."[49] Although the right to privacy has not been given a general definition, the EU has passed several directives to bring the right into the twenty-first century. For example, the 2002 E-Privacy Directive requires breaches of personal data to be reported to national authorities and may help provide a clearer picture on the actual number and scope of breaches in European countries.[50] Finally, the EU encourages the adoption of EHRs and confirmed the broad application of privacy protections.[51] These directives and suggestions promoted the access of information across various countries. While the

---

[47] John E. Dunn, *Europe Suffered 229 Public Data Breaches Since 2004*, IDG NEWS SERV. (Oct. 13, 2014), http://www.techcentral.ie/european-suffered-229-public-data-breaches-since-2004-study-suggests/ [http://perma.cc/3KCP-QJ8Z].

[48] *See* Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222, 230 [hereinafter Convention].

[49] H. Tomás Gómez-Arostegui, *Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations*, 35 CAL. W. INT'L L.J. 153, 154 (2005).

[50] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 [hereinafter E-Privacy Directive].

[51] Janine Hiller, et al., *Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared*, 17 B.U. J. SCI. & TECH. L. 1, 2 (2011).

United States also seems to be pushing to make EHRs the predominate form of record keeping through the HITECH Act, unfortunately they have not been able to promote patient privacy on the same level as the EU.

II. BACKGROUND

A. Development of the European Union's Right to be Forgotten

European and American ideas on individual privacy have gone in opposite directions. In 1950, the European Convention for the Protection of Human Rights and Fundamental Freedoms declared that, "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[52] In 1995, the EU made the Data Protection Directive into law, which includes the principal creating the right of erasure.[53] The right of erasure allows a subject to erase data, which is "incomplete, inaccurate, or stored in a way incompatible with the legitimate purposes pursued by the controller."[54] Additionally, Article 12 of the Data Protection Directive reads, "[m]ember states shall guarantee every data subject the right to obtain from the controller . . . as appropriate the rectification, erasure or blocking of data…."[55] Furthermore, Article 2 defines "controller," as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[56] The directive allows individuals some

---

[52] *See* Convention, *supra* note 48.

[53] *Factsheet on the "Right to be Forgotten" Ruling*, European Commission, (C-131/12), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf. [https://perma.cc/S33F-NWHA].

[54] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 32 [hereinafter EU Data Protection Directive].

[55] *Id.* at art. 12.

[56] *Id.* at art. 2.

control over the data that is processed by corporations and other entities.

The EU Data Protection Directive would have little to no authority if it did not apply to non-EU companies, and thus, it applies to any company that may reach within the EU. In 1991, the EU council adopted recommendations governing the flow of data across its borders.[57] The adoption of these recommendations is especially important when dealing with foreign companies possessing data of EU citizens.

Additionally, Article 8 of the EU Data Protection Directive prohibits the processing of personal data, "concerning health or sex life."[58] The EU Data Protection Directive formed the Article 29 Working Party, as an advisory board on data protection.[59] The Article 29 Working Party issued the Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records.[60] The report applies privacy principles to health records and "recommends [the] adoption of eleven specific legal protections to protect individual health privacy."[61] The report characterizes health data as being relevant to the treatment of the patient. Otherwise, it should not be included in the patient's medical file.[62] While these examples do not represent health data, they provide identifiable information that may trace de-identified health data back to the patient. Such information may hold relevance to a patient's history but often not to the patient's health. However, there are some exceptions where the information is extremely relevant. For example, a factory worker exposed to asbestos for thirty years will be relevant to the fact that the worker suffers from mesothelioma.

---

[57] *Recommendation No. R (91) 10 of the Committee of Ministers to Member States on the Communication to Third Parties of Personal Data Held by Public Bodies*, COUNCIL OF EUROPE (Sept. 9, 1991), *available at* https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=572401&SecMode=1&DocId=597936&Usage=2 [http://perma.cc/ N3RB-39HU].

[58] EU Data Protection Directive, *supra* note 54.

[59] Hiller, et. al, *supra* note 51 at 21.

[60] *Id.*

[61] *Id.*

[62] *Id.*at 22.

The EU system represents a huge victory for individual privacy rights by giving the individual control over what information the medical provider may collect and store. In 1980, the Organization for Economic Cooperation and Development ("OECD) issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines").[63] The OECD Privacy Guidelines operate on the principle of limiting data collection and use for only specific purposes.[64] It is noted that the guidelines put forth principles such as: "limitation of data collection, maintenance of data quality, specification of the collection purpose, limitation of data use to that specified purpose, adequate security, transparency, individual access to and control of data collected, and accountability."[65] In 1998, with the rapidly improving technological world the OECD reexamined the principles and reaffirmed their application.[66] However, OECD Privacy Guidelines remain limited in their application to health data. To protect individuals' health data, the European Union decided to address this issue.

In 2012, the European Union put forth a proposal to further protect individuals' privacy rights. The Proposal provides Article 17 the "Right to be forgotten and to erasure."[67] Three sections compose Article 17's right to be forgotten and to erasure. First, Section 1 provides individuals with the "right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in

---

[63] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris 1981), *available at* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/2RN8-P425].

[64] *Id.*

[65] Hiller, et. al., *supra* note 51 at 20.

[66] *See* OECD, *Protection of Privacy and Personal Data*, OECD.GOV, http://www.oecd.org/document/26/0,3343,en_2649_34255_1814170_1_1_1_1,00.html [http://perma.cc/K8LA-GGWK] (last visited on Feb. 7, 2016).

[67] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, COM (2012) 11 final (Jan. 25, 2012), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN [http://perma.cc/4ZY8-82A4] [hereinafter General Data Protection Regulation].

relation to personal data which are made available by the data subject while he or she was a child."[68] Section 2 includes the obligation of the controller who has made the information public to inform third parties of the data subject's request "to erase any links to, or copy or replication that personal data."[69] Section 3 charges the controller to take down the information "without delay" and creates exceptions where retention of personal data is necessary.[70] The exceptions include the exercise of "freedom of expression" such as works designated as artistic, literary, or journalistic; public health interest; "historical, statistical, and scientific research"; and retention of personal data by the EU or member state under state law.[71]

The General Data Protection Regulation was designed to meet the rapid advances in technology and provide individuals with protections against companies that make use of personal data.[72] The regulation's purpose is to build trust in the online environment to propel economic development; and as of April 14, 2016, the General Data Protection Regulation passed into law.[73] The right to be forgotten had little authority over the various corporations doing business in the EU, until 2013 when Spanish courts decided a case with immense implications to the right.

In 2013, the Spanish courts decided *Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez*. The decision required internet search engines to consider individual requests to remove links to freely accessible web pages resulting from a search of the individual's name.[74] The case was brought by a man

---

[68] *Id.* at art. 17.

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] Zlata Rodionova, *EU Data Protection Regulation Passes in Brussels Giving Citizens Right to be Forgotten Online,* (April 14, 2016), http://www.independent.co.uk/news/business/news/european-union-s-general-data-protection-regulation-privacy-facebook-data-eu-law-online-web-a6984101.html. [https://perma.cc/3RQX-4XTU].

[74] Case C-131/12, Google Spain SL v. Agencia Española de Proteccion de Datos, (AEPD), 2013 ECLI:EU:C:2014:616 (May 13, 2014), *available at*

whose name was printed in an announcement of a newspaper widely circulated throughout Spain in connection with a property that was up for auction due to Social Security debts.[75] The man was named as the owner.[76] At a later date, an electronic version of the newspaper was made available.[77] In 2009, the man searched for his name on Google and found the newspaper announcements from eleven years prior.[78] The man asserted Article 12 of the EU Data Protection Directive as the basis of his argument to require Google to erase the search results.[79]

In its decision, the court reasoned that while the General Data Protection Regulation in Article 17 provides for a right to be forgotten, it does not represent a codification of current law.[80] However, the court did find that the right of erasure is valid when Google, acting as a processor of personal data, infringes on the privacy rights of the data subject.[81] The decision gives real authority to the EU Data Protection Directive Article 12, recognizing the right to erasure in the EU common law. Furthermore, the decision requires U.S. companies to adhere to this right to be forgotten when operating within the EU. It remains to be seen the impact this will have on U.S. companies' operations within the EU and if the right to be forgotten will impact the companies' data policies within the United States.

The *Google Spain SL* decision draws parallels to the United States' Supreme Court decision in *Griswold v. Connecticut* which began the constitutionally recognized right of privacy in the United States.[82] In *Griswold*,

---

http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [perma.cc/9M35-KEV6] [hereinafter Google Spain].

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.* (asserting in the complaint by Mr. Gonzalez that the proceedings that gave rise to the announcements had been resolved several years prior and were no longer relevant. The, though the court found that the newspaper publishing the announcements were right to do so but upheld the complaint against Google Spain and Google, Inc.).

[80] *Id.*

[81] *Id.*

[82] Griswold v. Connecticut, 381 U.S. 479 (1965).

Connecticut had a statute that mandated any individual be fined who used "any drug, medicinal article or instrument for the purpose of preventing conception."[83] Griswold, the Executive Director of the Planned Parenthood League of Connecticut, provided information and drugs to married persons for the "purpose of preventing contraception."[84] She was subsequently fined for her actions.[85] The Court found the Bill of Rights and its Amendments create "zones of privacy."[86] For example, the Fourth Amendment provides an individual's right from "unreasonable searches and seizures" of their homes.[87] The Court found the constitutionally guaranteed zones of privacy extended to marital privacy.[88] *Griswold*, much like *Google Spain* in the EU, represents the beginning of constitutionally protected privacy rights in the United States.

In applying the EU Data Protection Directive to the health care industry, Article 29 of the Data Protection Working Party is dispositive for the EU health care industry. Under Article 29, the Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records provides requirements for health information gathered by health care professionals in electronic form.[89] Health information gathered must be for the purposes of "preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services" the health professional processing the information must be bound by law or professional rules to professional secrecy or the 'equivalent.'[90]

---

[83] *Id.* at 480 (citing now repealed CONN. GEN. STAT. § 54-196 (1958)).

[84] *Id.*

[85] *Id.*

[86] *Id.* at 484.

[87] *Id.* at 484.

[88] *Id* at 485. The constitutionally guaranteed zones of privacy are no longer applicable. In subsequent cases the zones of privacy have been replaced and a right to privacy has been founded in the 14th Amendment's Due Process Clause. *See* Roe v. Wade, 410 U.S. 113 (1973), note 96.

[89] Article 29 of Directive 95/46/EC, Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR), 2007 O.J. (WP 131), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf [http://perma.cc/E6SY-95PA] [hereinafter Article 29].

[90] *Id.*

The EU created eHealth as its electronic health record database.[91] The eHealth database provides Europeans with access to their medical data while incorporating the right of individuals to have their medical data safely stored on an accessible online health care system.[92] European EHRs require prior patient consent, but once given, providers can freely access, store, and transmit the information.[93] The main obstacle to eHealth's success is concern over data protection and privacy.[94] Similar to the concerns in the United States electronic health record system, in the EU "there is still lack of trust in the security of the system and [patients] are reluctant to use it."[95] This distrust stems from a concern over access to the information.[96] Additionally, patients and providers express concerns on data privacy but also concern on "overly strict data protection."[97] To combat these concerns, the eHealth stakeholders put forth recommendations as to how to properly secure patient information.[98] One recommendation, guaranteeing privacy and data protection, grants patient's control over their own medical file.[99] The patient is in charge of his or her own file, allowing the patient to "log-in" and inspect it.[100] The EU finds the option to access one's own information as a fundamental right under the EU Data Protection legislation.[101] The United States should grant patients

---

[91] Directive 2011/24/EU, of the European Parliament and of the Council of 9 March 2011 on the Application of Patients' Rights in Cross-Border Healthcare O.J. (L 8845) [hereinafter Directive on Cross-Border Health care].

[92] PATIENT ACCESS TO ELECTRONIC HEALTH RECORDS, EHEALTH STAKEHOLDER GROUP, 1 (2013), *available at* http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5169 [http://perma.cc/8G6P-YNWQ] [hereinafter EHEALTH REPORT].

[93] *Id.* at 2-3.

[94] *Id.*

[95] *Id.* at 3.

[96] *Id.* Most concern is over the "who and how" of data access. Stakeholders remain tentative, because EHRs carry a general uncertainty of who is responsible for the information.

[97] *Id.* at 4.

[98] *Id.* at 14.

[99] *Id.*

[100] *Id.*

[101] *Id.*

similar access to their own files. This way the patient will have the opportunity to become more involved in their recordkeeping and have some sense of security even if it is small.

However, it is argued that "an EHR in the United States will challenge the presumption of privacy preservation."[102] With records easily transferable between providers, the individual's ability to maintain privacy is limited. This is a problem in the EU as well, but if the recommendations presented by eHealth take hold, then the patient will be able to see who accessed their information and for what purpose.[103] Yet, with the increase in medical data breaches, EHRs should strengthen the presumption of privacy. If the United States health care industry cannot protect health records, then the decision of what non-treatment related information is in the records should be made by individuals.

B. Development of the United States' HIPAA Law

The United States codified its concern for privacy in the various Amendments constituting the Bill of Rights. For example, the Fourth Amendment protects against unreasonable search and seizures[104] and the First Amendment's freedom of association.[105] With *Griswold v. Connecticut*, the seminal case on U.S. privacy rights, the Supreme Court recognized a constitutional right to privacy.[106] *Griswold* began a snowball effect for privacy rights, including *Roe v. Wade*[107] and *Cruzan v. Director, Missouri Department of Health*.[108] However, the Court has

---

[102] Hiller, et al., *supra* note 51 at 23.

[103] EHEALTH REPORT, *supra* note 92.

[104] U.S. Const. amend. IV.

[105] U.S. Const. amend. I.

[106] Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

[107] Roe v. Wade, 410 U.S. 113 (1973). In this right to abortion case, the Court found "the right [of privacy]…includes the right of a woman to decide whether or not to terminate her pregnancy." *Id.* at 170.

[108] Cruzan v. Dir., Mo. Dep't of Health, 497 U.S. 261 (1990). In this end of life case, the Court assumed a person's right to refuse treatment to be a liberty interest (a right not to be infringed upon by the government, state or federal) protected by the Due Process Clause and

not recognized a constitutional right to privacy of health data.

In *Whalen v. Roe*, the Supreme Court recognized a limited Constitutional right to individual privacy with respect to information held in government databases.[109] However, the decision left unresolved the issue of a constitutional protection of health information. With the Privacy Act of 1974, Congress created a law that applies to personal information in any federal government record within federal agencies.[110] Then, with the Gramm-Leach-Bliley Financial Services Modernization Act of 1999, Congress protected financial information held by health insurers.[111]

Wanting an expanded right to privacy yet to be court recognized within the various constitutional amendments, Samuel Warren and Louis Brandeis wrote that there should be a right "to be let alone" from instantaneous photographs and newspaper enterprise invading the private and domestic life.[112] However, the Supreme Court did not recognize the right to privacy within the Bill of Rights until much later.[113] Congress was the first to act to protect privacy rights regarding health data.[114]

Health Insurance Portability and Accountability Act of 1996 ("HIPAA") started the United States' move toward EHRs. The U.S. legal framework for health information privacy is codified in HIPAA.[115] HIPAA "originally gave Congress three years to pass explicit privacy rules."[116] After

---

went through a Due Process Clause analysis weighing the state interests against Cruzan's liberty interests. *Id.* at 279.

[109] Whalen v. Roe, 429 U.S. 589 (1997).

[110] Privacy Act of 1974, 5 U.S.C. § 552a (2016).

[111] Gramm-Leach-Bliley Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat 1338.

[112] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[113] Griswold v. Connecticut, 381 U.S. 479, 481 (1965) (deciding the right to contraception was a privacy right found within the constitutional amendments, but later the right to privacy is found in the Due Process Clause of the 14th Amendment).

[114] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1997) (codified as amended in various sections of 42 U.S.C.).

[115] *Id.*

[116] Hiller, et al., *supra* note 51 at 11.

this time expired and no privacy rules were passed, the Department of Health and Human Service ("HHS") "became the authority in privacy regulations."[117]

HIPAA was a congressional attempt to provide administrative simplification of the health care system through a health information system with the electronic transmission of certain health information.[118] HHS began to adopt a set of rules to govern health information privacy with the Privacy Rule.[119] The Privacy Rule has three purposes best described in three words: protect – safeguard the rights of consumers "by providing them access to their health information" and restricting the inappropriate use; trust – "improve the quality of health care" by "restoring trust" between those supplying and seeking health care; improve – develop a "national framework for health privacy protection" to improve "efficiency and effectiveness." [120]

Next, the HHS passed the Security Rule. The Security Rule creates standards for the measures to be taken when "covered entities" obtain custody of health information. These standards apply to communication of health information between "covered entities" and "business associates."[121] Section 160.103 of the Federal Regulations defines covered entity to mean "(1) a health plan[,] (2) a health care clearinghouse[, and] a health care provider who transmits any health information in electronic form."[122]

In 2009, Congress strengthened HIPAA's privacy and security rules through the HITECH Act. HITECH also clarified the business associate requirements.[123] HITECH defines business associate as "a person who on behalf of such covered entity or of an organized health care arrangement in

---

[117] *Id.*

[118] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in various sections of 42 U.S.C.).

[119] *Id.*

[120] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

[121] Health Insurance Reform: Security Standards Final Rule, 68 Fed. Reg. 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, 164).

[122] 45 C.F.R. §160.103 (2010).

[123] *Id.*

which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information."[124] The HITECH Act increased the strength of HIPAA's privacy security guidelines by increasing enforcement and civil monetary penalties.[125] Enforcement and civil monetary penalties increased in strength with the Breach Notification Rule codified within 45 C.F.R. §§ 164.400-14.[126]

The Breach Notification Rule requires "covered entities" and business associates to notify the individual affected in cases of 500 or less, but the local media must be informed when 500 or more residents of a state are affected by a breach.[127] Also, the rule allows the Secretary of HHS to post on the HHS public website the names of each covered entity involved in a breach of more than 500 individuals.[128] For example, the Community Health Systems ("CHS"), Inc. breach affected 4.5 million people, and CHS is posted on the HHS public website.[129] Applying the heightened civil penalties under the HITECH Act, CHS could be fined millions of dollars by HHS.[130]

The breach was a result of a Chinese cyberattack that affected 4.5 million patients.[131] Despite the fact that no health-related information was stolen, the stolen information included identifiable data such as birthdates and telephone numbers.[132] Although stolen in a sophisticated attack, this leak of information still constitutes a breach under HIPAA.[133] According to the HIPAA breach notification rule, HHS

---

[124] *Id.*

[125] Hiller, et al., *supra* note 51 at 12.

[126] 45 C.F.R. §§ 164.400-14 (2013).

[127] 45 C.F.R. § 164.408 (2013).

[128] *Id.*

[129] Munro, *supra* note 14.

[130] *Id.*

[131] Nicole Perlroth, *Hospital Company Hacked, Affecting 4.5 Million Patients (Hack of Community Health Systems Affects 4.5 Million Patients)*, N.Y. TIMES, (Aug. 19, 2014), *available at* http://bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients/?_r=0 [https://perma.cc/RH7T-SVQJ].

[132] *Id.*

[133] Munro, *supra* note 14.

required CHS to contact the patients and notify HHS because it affected more than 500 individuals.[134]

In working through the details of HIPAA and understanding protected health information, one must understand the role played by covered entities and business associates. Originally, HIPAA only regulated covered entities with regards to protected health information.[135] It completely left out entities essential to the exchange of health information, i.e. business associates.[136] Subsequent changes to the HIPAA law broadened its application to business associates, and the HITECH strengthened its enforcement against business associates involved in a data breach.[137]

HIPAA goes on to distinguish between two types of disclosures: permissive and required disclosures. "Required disclosures include a covered entity's provision of a patient's own protected health information to the patient or patient's representative, and requests by the HHS secretary for PHI for audit or enforcement."[138] On the other hand, permissive disclosures are all other disclosures that fit two categories: those without patient authorization and those that require patient authorization.[139] Disclosures without patient authorization include exchanges between providers regarding the treatment of a patient and billing for services.[140] Disclosures requiring patient authorization include exchanging information with the patient's

---

[134] *See* 45 C.F.R. § 164.408 (2013).

[135] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in various sections of 42 U.S.C.).

[136] Hiller, et al., *supra* note 51 at 121.

[137] With the expansion of EHRs in the last decade, this change to HIPAA has helped bring accountability to organizations that may contribute to a breach, but patients deserve heightened rights to protect their own data. *Id.* at 12-14.

[138] Melissa Goldstein, Lee Repasch & Sara Rosenbaum, *Chapter 6: Emerging Privacy Issues in Health Information Technology,* in HEALTH INFORMATION TECHNOLOGY IN THE UNITED STATES: WHERE WE STAND 97 (David Blumenthal et al. eds., 2008), *available at* https:// folio.iupui.edu/bitstream/handle/10244/784/hitreport.pdf [http:// perma.cc/ SSE5-BUHS].

[139] *Id.*

[140] *Id.*

representative and requests by the HHS for enforcement purposes.[141]

Protected health information means "individually identifiable health information" that is held or transmitted by a covered entity in any form or media.[142] Patient authorization is required when the provider is receiving some form of remunerations for the exchange.[143] However, no authorization is required to share health information when being treated, securing payment, or in performing health care operations.[144] Disclosure should be limited to the "minimum necessary."[145] A covered entity may share de-identified information to help improve the public's understanding of the quality of health care.[146]

Under HIPAA, enforcement is left to the Secretary of HHS. There is no private right of action under HIPAA (federal law).[147] Some states provide a private cause of action[148] under state HIPAA- type statutes, such as California, for example.[149] This represents a conscious decision on the part of Congress to favor the exchange of protected health information over patient privacy rights.[150]

Only HHS has jurisdiction to enforce HIPAA and seek penalties for HIPAA violations. HIPAA violations can include

---

[141] *Id.*

[142] 45 C.F.R. § 160.103 (2010).

[143] SUMMARY OF THE HIPAA PRIVACY RULE, U.S. DEP'T OF HEALTH & HUMAN SERVICES, SUMMARY OF THE HIPAA PRIVACY RULE at 3 (2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[144] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13405(d), 123 Stat. 115, 264 (2009).

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *See* Daniel J. Gilman & James C. Cooper, *There is a Time to Keep Silent and a Time to Speak, The Hard Part is Knowing Which is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279, 302, 309 (2010).

[149] For example, the California HIPAA-type statutes regulate the disclosure of medical information by providers and actions that can be brought by unlawful disclosure of patient information. CAL. CIV. CODE § 56.10-16 (2014).

[150] *See id.*

civil and potentially criminal penalties.[151] There are differing degrees of penalties depending on the intent of the violation.[152] Penalties can be levied against both business associates and covered entities.[153] Enforcement examples can be seen on the HHS website where companies are listed that had a breach affecting more than 500 individuals.[154]

However, individuals should have a private right of action at the federal level. It is their health information that is being mishandled and stolen. They are suffering harm that may become irreparable. Stolen personal information can lead to identity theft. Identity theft can ruin an individual's credit score and lead to financial losses when the theft includes Social Security numbers and birth dates. For medical identity theft, it could lead to confusion of medical history along with financial loss. Moreover, none of these risks are confined by state borders.

After seeking treatment for an ailment, no one wants to have to worry about someone stealing that information. Health care corporations and the government must take extra steps to protect health records or give individuals the right to determine when and what nontreatment-related information is included in them.

III. ANALYSIS: APPLYING EUROPE'S RIGHT TO BE FORGOTTEN TO AMERICANS' HEALTH RECORDS

A. What an American Health Care Privacy Right to be Forgotten Might Look Like

In general, the EU has continuously provided greater individual privacy rights than the United States.[155] It is time

---

[151] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13410 (a), 123 Stat. 115.

[152] *Id.*

[153] *Id.*

[154] 45 C.F.R. § 164.408 (2013).

[155] Bob Sullivan, *'La Difference' is Stark in EU, U.S. Privacy Laws*, NBC NEWS, (October 19, 2006), http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.V0Hn-_krLIU. [https://perma.cc/HJ33-XTMT]. *See also* Convention, *supra* note 48. *See also* Article 29, *supra* note 91. *See* Directive on Cross-Border Healthcare, *supra* note 90. *See* EU Data Protection Directive, *supra* note 53.

the United States acknowledged individual privacy rights and addressed the recent increase in data breaches by offering greater protection to individuals. To address the United States' lack of health information privacy rights, the government should consider the following steps: explicitly recognize a right to data privacy; pass legislation that strengthens HIPAA enforcement granting a private right of action on the federal level; adopt a right of erasure for health data found acceptable to be removed by HHS through administrative notice and comment proceedings; and grant a right to be forgotten in HIPAA for information that is breached and released onto the Internet.

Step One: As the United States Supreme Court has recognized the right to privacy as a fundamental right similar to the EU's right in their European Convention for the Protection of Human Rights and Fundamental Freedoms,[156] the United States needs to pass legislation that would grant an explicit right of privacy for personal data. An American right to data privacy should be similar to a right to privacy found in the French Civil Code. In Article 9, the French Code provides for the right to respect of one's private life[157] French courts have interpreted private life to mean "love life, friendships, family circumstances, leisure activities, political opinions, trade, union or religious affiliations, and state of health."[158] Acknowledgement of such a right in the United States would allow Americans an opportunity to have autonomy over their personal and private data.

Step Two: Pass legislation that strengthens HIPAA enforcement. Legislation should allow a private right of action against HIPAA violators in federal court. Under paragraph two of Article 9 in the French Civil Code, the court is given the necessary measures to stop those infringing on others' privacy.[159] The United States should address data breaches as an infringement on the patients' privacy. HIPAA

---

[156] *See* Convention, *supra* note 48.

[157] CODE CIVIL [C. CIV.] art. 9 (Fr.).

[158] *French Legislation on Privacy*, EMBASSY OF FRANCE IN WASHINGTON (Dec. 2, 2007), http://ambafrance-us.org/spip.php?article640 [http://perma.cc/N7ZK-VJSC].

[159] *Id.*

should provide more specific requirements on the level of transparency between covered entities and individual patients when collecting data. More transparency would give patients a better opportunity to make an informed decision.

Step Three: Adopt comparable measures listed in the EU Data Protection Directive. The Directive applies to non-EU companies as seen in *Google Spain*[160] and, since United States' companies are already exposed to the right, a transition would not be that difficult.[161] Legislation should place the protection of data and the free access of information on a level playing field.[162] The United States should adopt a right of erasure that ensures health information no longer relevant to an individual will be removed from certain domains similar to the right found in the proposed European Directive.[163] For examples, doctors who contracted the Ebola virus while working in West Africa and returned home to be cured will not have their reputation tarnished by the information remaining on the Internet. Data becomes susceptible to exposure when it reaches a digital form, this liquidity allows for quick travel among thousands of people, versus one person viewing a paper record they were not supposed to see. It is my proposition that the right to erasure be tested on outdated and irrelevant Internet pages and then implemented into EHRs after trial and error with a right that applies to the Internet.

---

[160] In the *Google Spain* decision, the court addressed the territorial issues of the EU Data Protection Directive and affirmed its application to non-EU corporations collecting and storing personal data for advertisement purposes within the EU territories such as Google, Inc. Case C-131/12, Google Spain SL v. Agencia Española de Proteccion de Datos, (AEPD), 2013 ECLI:EU:C:2014:616 (May 13, 2014), at paragraph 60-68.

[161] With the proposed EU General Data Regulation, United States businesses will be subject to EU privacy laws, even though they are located outside of EU territories if they are collecting and storing an EU citizen's personal data. *European Union Imposes Extraterritorial Privacy Obligations on U.S. Businesses*, THOMPSON HINE (May 16, 2014), http://www.thompsonhine.com/publications/european-union-imposes-extraterritorial-privacy-obligations-on-us-businesses [http://perma.cc/Z5G5-NJMF].

[162] EU Data Protection Directive, *supra* note 53.

[163] *Id.*

Step Four: Incorporate into HIPAA the EU's proposal for a right to be forgotten. HIPAA does not recognize a private right of action, and incorporating the EU's proposal for a right to be forgotten would give patients' full autonomy over their health information.[164] A private right of action would provide individuals an opportunity to protect their reputation during a breach.[165] The proposed right to be forgotten empowers individuals to assert greater control over their reputations and identities on the Internet.[166] The controversial right would grant individual citizens the ability to demand the permanent removal of personal content from the Internet.[167] There is an argument that this proposed right would have a negative impact "on freedom of expression and notions of privacy"[168]; however, such a right strengthens these freedoms by allowing revocation of certain expressions, like a painter painting over one of his pieces of artwork.[169] An individual who mistakenly posts on a social media site should have the ability to permanently delete the post from the Internet. Similarly, it allows minors accessing the Internet via social media to erase potentially reputation-destroying posts.

One may ask how this right to be forgotten will apply to EHRs? The right should be applied when a patient no longer seeks care from a certain provider. If the patient has made an affirmative action to see another provider, once the EHR is passed to the new provider, then the patient should have the right to erase the EHR from the prior provider. Additionally, irrelevant health information should be available to the right as well. HHS will play a vital role in determining which health information may be available.[170]

---

[164] *Id.*

[165] Emily Adams Shoor, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation*, 39 BROOK. J. INT'L L. 487, 489 (2014).

[166] Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. 88 (2012).

[167] Shoor, *supra* note 168.

[168] *Id* at 487.

[169] *Id.*

[170] HHS rulemaking must be done through notice and comment proceeding under the Administrative Procedure Act. Ideally this approach would allow experts to weigh in on the issue and allow HHS to

Empowering patients to control their own health information may lead to better outcomes, although there is no evidence to support this proposition.

Another possible way to protect patient data may be through the Consumer Privacy Bill of Rights Act, a draft bill proposed by the Obama administration.[171] As Nicolas Terry, a professor at Indiana University Robert H. McKinney School of Law, states, the bill goes further than current HIPAA regulations in requiring custodians to furnish a more encompassing privacy policy.[172] Additionally, the bill "presupposes some consent mechanism (removed from HIPAA in 2002) and provides for withdrawal of consent and, in some situations, erasure."[173] The Consumer Privacy Bill of Rights is a step in the right direction for the Obama administration and begins the all too important first step in the realization of a right of health data privacy mentioned within this Note.

B. Problems With An American Right to be Forgotten

Implementation of the right to be forgotten would be a difficult, but not impossible, endeavor for the United States. The right to be forgotten would have to be a legislatively-created right and the statute constitutionally permissible. The United States courts, legislature, and even the Constitution have not given an explicit right to privacy for electronic health data. While the European Union's right to

---

make a rule that is as well tested as possible. *See* Administrative Procedure Act, 5 U.S.C. § 553 (2015).

[171] Nicolas Terry, *Should Health Lawyers Pay Attention to The Administration's Privacy Bill?*, HEALTH AFFAIRS (Mar. 13, 2015), http://m.healthaffairs.org/blog/2015/03/13/should-health-lawyers-pay-attention-to-the-administrations-privacy-bill/ [http://perma.cc/CA3U-ABX3] (discussing the Consumer Privacy Bill of Rights Act and its potential application to the health care industry).

[172] *Id.*

[173] *Id.* Professor Terry illustrates the difficulty in the United States allowing data minimization in the health care industry. Currently, we operate under a system that supports the transferability of data. Professor Terry argues that the greatest impact will be felt by "big data brokers and [health] app developers."

be forgotten stays within the realm of data privacy[174] and not health information, the United States form should encompass both.

Furthermore, the United States' courts have not recognized a right of privacy for health information that the right to be forgotten would require.[175] A health information right of privacy would grant individuals autonomy over what health information appears on the Internet and what non-treatment information is in the health records. Bipartisanship support in the United States legislature has proven difficult to attain. Thus, getting such a right passed through both houses and signed into law by the President may prove an immense challenge. Once passed, the implementation could take years before the right is fully available to individuals.[176] First Amendment proponents will attack the right as a way to diminish the freedom of speech and expression.[177]

The EU has not been immune from free speech arguments against their right to be forgotten. The defense was raised after the European Court of Justice issued the *Google Spain* decision.[178] The EU saw two very different principles collide: the right of privacy and the freedom of speech.[179] It reconciled the two rights by limiting removal of information to "inaccurate, inadequate, or no longer relevant" personal information.[180] However, the European Court of Justice failed to provide definitions to these terms.[181] The United

---

[174] General Data Protection Regulation, *supra* note 68.

[175] Whalen v. Roe, 429 U.S. 589, 605-06 (1977).

[176] Joel Reidenberg, *Restoring American's Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 787 (1999).

[177] *See* Shoor, *supra* note 164, at 498-500.

[178] Luciano Floridi, *Should You Have the Right to be Forgotten On Google? Nationally, Yes. Globally, No.*, HUFFINGTON POST, http://www.huffingtonpost.com/luciano-floridi/google-right-to-be-forgotten_b_6624626.html [http://perma.cc/2TGK-ZNMT] (last updated Apr. 7, 2015).

[179] *Id.*

[180] *Id.*

[181] Opponents of the decision are worried about its effects on freedom of expression, especially in the context of journalistic and artistic expression. They continue by pointing out that the court failed to explain the right to be forgotten's application to the other fundamental rights, such as the freedom of expression. Eleni Frantziou, *Further*

States Constitution protects the freedom of speech, [182] which poses an even larger hurdle for a statutorily created right to electronic data privacy. However, Congress may pass a constitutionally permissible statute allowing a right to electronic data privacy if it is similarly narrowly defined and does not infringe on the freedom of speech.[183] A right to electronic data privacy could look similar to the common law doctrine of informed consent. Informed consent provides that physicians will make a guideline as to what information the patient needs to make a reasonable decision regarding their treatment.[184] A right to electronic data privacy will require the provider to disclose to the patient where and what data will be electronically transferred. Similar to informed consent, it will require the patient to agree to the transfer of the data between "covered entities" and "business associates."[185]

Once implemented, HHS will have to decide which parts of a patient's health information will be available to be "forgotten." Any information that is not relative to a current treatment and anything past six years should be subject to the right. HHS will determine which information is available by a notice and comment rulemaking procedure.[186] HIPAA holds a similar retention period for its policies and procedures.[187] For example, someone with high blood pressure would not be able to erase any data related to the patient's heart health. However, a patient who was cured of an ailment or a symptom should be able to have that

---

Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc. v Agencia Espanola de Proteccion de Datos, 14 HUM. RTS. L. REV. 761, 767 (2014).

[182] U.S. CONST. amend. I.

[183] *See* Floridi, *supra* note 177.

[184] *See generally* Canterbury v. Spence, 464 F.2d 772 (1972).

[185] *Id.*

[186] This procedure could include looking at allowing patients to revoke all consent for providers to collect and store their information, or it could include patients being able to remove certain ailments such as a sprained ankle that experts feel may not affect other ailments. Administrative Procedure Act, 5 U.S.C. § 553 (2015).

[187] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in various sections of 42 U.S.C.).

information forgotten until the patient is ready to disclose it. Merriam-Webster Dictionary defines cure as "recovery or relief from a disease,"[188] and symptom as "a change in the body or mind which indicates that a disease is present."[189] However, the HHS department will likely need to create a board with members appointed by the President to determine which symptoms and ailments will be available for removal. The President has the power of appointment under Article II of the Constitution[190] to appoint leading minds in the medical field to the board. Community insight from the notice and comment requirements under the Administrative Procedure Act could be a valuable tool in determining the ailments and diseases to be subject to the right.[191]

Further, the patient will have the ability to revoke consent to the transmission of their information at any time in the health care delivery system. Every company with access to protected information will be subject to HIPAA right to be forgotten, and must relay notification of their access to such data to each individual.

Push back from "covered entities" and "business associates" in the health care industry will be significant. The health care industry will likely argue that the past legislation has pushed them to have electronic health records be more accessible, whereas this would attempt to restrict the free flow of records.[192] Providing a private right of action for violations of the right to be forgotten and subsequent data breaches would place added liability on these health providers.[193] This will likely lead to an increase in health care costs in the U.S. However, the higher costs to a strengthened HIPAA will ideally reflect in lower fraud costs. Once the

---

[188] *Cure Definition*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/cure [http://perma.cc/59L5-3LFB] (last visited Feb. 7, 2016).

[189] *Symptom Definition*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/symptom [http://perma.cc/YRU8-ZMW6] (last visited Feb. 7, 2016).

[190] U.S. CONST. art. II, § 2.

[191] Administrative Procedure Act, 5 U.S.C. § 553 (2015).

[192] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in various sections of 42 U.S.C.).

[193] Shoor, *supra* note 164 at 491.

system is in effect, then costs will likely fall, and fraud costs will remain at a low rate. Another provider criticism will point to the lack of patient awareness or patients not being informed enough to make reasonable decisions on what information to erase.[194] While this may always be the case with some patients, educating the population may be able to increase patient awareness and use of the right.

The EU model for the right of erasure and right to be forgotten places the onus on the consumer (in this case the patient) to make an informed decision.[195] This could prove difficult for an American populace that has historically been far removed from the health delivery system. Patients can become quickly overwhelmed when asked to make a medical decision on their own,[196] however, a push for more health care education regarding price and options should be available. Patients also rarely know the prices of the treatment they receive beforehand. This lack of knowledge is largely due to the third party payer system the United States has adopted. Today, patients under HMOs have very little say in their own health care. The HMOs provide a list of physicians and networks in which the patient may choose.[197] The average patient will have little choice but to accept what the HMOs have already decided for them.[198] The cost of health care will continue to rise under such a system, because the patient is far removed from the payment process.

C. Solutions

First for such a plan to work, the legislature must recognize a right to electronic data privacy of the individual.

---

[194] Reed Abelson & Julie Creswell, *Report Finds More Flaws in Digitizing Patient Records*, N.Y. TIMES (Jan. 8, 2014) *available at* http://www.nytimes.com/2014/01/08/business/report-finds-more-flaws-in-digitizing-patient-files.html?_r=0 [http://perm.cc/ SJK4-9J4W].

[195] General Data Protection Regulation, *supra* note 68.

[196] Jan Hoffman, *Awash in Information, Patients Face a Lonely, Uncertain Road*, N.Y. TIMES (Aug. 14, 2005), *available at* http://www.nytimes.com/2005/08/14/health/14patient.html?pagewanted=all&module=Search&mabReward=relbias%3Aw%2C%7B%222%22%3A%22RI%3A14%22%7D [http://perma.cc/V84D-6V26].

[197] *Id.*

[198] *Id.*

As a society, we must continue to push for greater data privacy rights. The right to electronic data privacy encompasses the requirement of consent for nontreatment-related information in a patient file and the removal of articles and health-related posts on social media. Such a right should be granted to all individuals. A right to electronic data privacy allows individuals autonomy over what information is disclosed to the public rather than third party corporations.[199]

Second, the ACA's push for a national electronic health records system must be realized.[200] This would improve the accessibility, effectiveness and security of electronic health records. It would also allow for easy removal of unnecessary information from patient records.[201] For example, a patient who removes consent to a provider holding nontreatment related information such as the patient's birthdate or Social Security Number. Once the patient pays his or her bill for the services provided, the patient will have the opportunity to remove that information from their file. In this way, the patient is afforded some protection in case of a data breach.

Under the HITECH act, Congress provided for billions of dollars in incentives for physicians and hospitals to move to electronic health records.[202] However, with vast amounts of health care providers' records not on the same system, the easy flow of information from one system to another has proven to be difficult.[203] Further, Congress failed to understand how valuable medical information was to hackers and identity thieves. Networks are not protected nor compatible to move information.[204] For security to properly

---

[199] Shoor, *supra* note 164.

[200] *Key Features of the Affordable Care Act By Year*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/healthcare/facts-and-features/key-features-of-aca-by-year/index.html [http://perma.cc/23S6-UMYX] (last updated Aug. 13, 2015).

[201] *See* Abelson & Creswell, *supra* note 194.

[202] 42 U.S.C. § 300jj-31 (2016).

[203] Julie Creswell, *Doctors Find Barriers to Sharing Digital Medical Records*, N.Y. TIMES, (Sept. 30, 2014)http://www.nytimes.com/2014/10/01/business/digital-medical-records-become-common-but-sharing-remains-challenging.html [http://perma.cc/6JGR-YNHA].

[204] *See id.*

protect health records, the exchange system must be properly tested and run smoothly. Employees operating the system must be adequately trained, as the most common form of data breach is employee related.[205] Employee breaches include lost or stolen computer equipment and "unintentional employee action."[206] Even though rigorous employee training accidents will still occur, the government can mitigate and limit the number of accidents.

In Britain, they attempted a similar national health electronic records system, but it failed.[207] British Parliament attempted to install such a system without working with health care providers.[208] It appears that the current United States attempt to install a national system of electronic health records will fail without a cohesive effort by everyone involved.[209] A national system of electronic health records could prove a valuable defense against hackers and medical identity thieves. For such a system to work, health care providers, legislators, and electronic health tech companies would have to work hand in hand. Otherwise, electronic health records will continue to have problems in exchanges.

There needs to be more transparency in the health care system. Patients are disconnected from the health care system.[210] Patients have limited autonomy outside of choosing whether or not to adhere to a treatment plan.[211] Patients are not given enough information to determine which provider to attend or what procedure is most effective.[212] Along with needing more information on data privacy, the American system of third party payers leaves many patients unaware of treatment costs. Data regarding

---

[205] Bendix, *supra* note 42.

[206] *Id.*

[207] Steve Lohr, *Lessons from Britain's Health Information Technology Fiasco*, N.Y. TIMES BITS BLOG (Sept. 27, 2011, 7:40 AM) http://bits.blogs.nytimes.com/2011/09/27/lessons-from-britains-health-information-technology-fiasco/?module=Search&mabReward=relbias%3Aw%2C%7B%222%22%3A%22RI%3A14%22%7D/ [http://perma.cc/58Y3-4H4V].

[208] *Id.*

[209] *Id.*

[210] Abelson & Creswell, *supra* note 194.

[211] Hoffman, *supra* note 196.

[212] *Id.*

care and privacy needs to be readily available to the average layperson in order for them to make an informed decision.

IV. CONCLUSION

The United States must address its lack of individual privacy protections. The United States needs to address the lack of health data privacy protections. In today's technological world, individual privacy rights must be strengthened to the point individuals can trust providers to keep their information safe. American citizens should have the right to be forgotten rather than have their information lost or stolen.

Similarly, technology is constant and everywhere in today's world, and the United States has provided limited protections to personal data. The United States must move quickly towards a legislative solution to solve the data protection issues facing the nation.[213] The current EU Data Protection Directive took five years to implement.[214]

The United States should adopt the EU's right of erasure to protected health information. A right of erasure would require extensive cooperation between the two political parties to adopt such a differing stance on privacy rights.[215] A right of erasure would allow patients complete control over the transmission of their information, along with the ability of patients to revoke consent to providers collecting and storing their information. Such a right would also allow patients to erase prior treatments, ailments, and symptoms that are no longer related to the patients care. For example, after the Ebola crisis, patients should not have to keep in their records retained by their health care providers that they were diagnosed with the virus.

---

[213] Reidenberg, *supra* note 176, at n.1. (examining surveys that show ". . . 82 % of those surveyed feel that consumers have lost all control over how companies collect and use their personal information.").

[214] *Id.* at 787.

[215] *See generally* Terry, *supra* note 171. (explaining the changes under the 1015 draft bill). Under the Democratic Obama administration, the 2015 Consumer Privacy Bill or Rights Act will extend HIPAA to greater protect health data, but it is yet to be passed in a Republican-controlled Congress.

Kaci Hickox returned from West Africa aiding the nations stricken most severely by the Ebola virus.[216] Upon her return and an elevated temperature at the airport, Hickox was quarantined by airport officials and required to stay home for a 21-day period.[217] She engaged in a public fight with Maine officials over whether her travel after the 21-day monitoring period should be restricted.[218] Even though she won, her name will remain on the Internet for years to come. Patients like Kaci Hickox should have the right to be forgotten.

The Obama administration's Consumer Privacy Bill, or Rights Act, is an important first step for the United States toward a right to be forgotten. Data privacy is increasingly becoming a major issue in the both political and economic spheres of the country.[219] It is important to solidify the right to health data privacy to protect against the ever-present threat of cybercriminals.

Imagine once more Jane Doe waking to a breaking story on the news that her health insurance provider's system was the victim of a cyberattack. However, Jane rests easy, because she can exercise her right of erasure and her right to be forgotten, and her highly sensitive health data and private information may be removed with a click of a button. These rights place the power to access, collect, and store this information where it should be, in the individual's hands. The health care industry has continually failed to protect individuals' information, and it is time the United States has addressed the issue with stronger protections for individual data privacy.

---

[216] Dana Ford, *Ebola Nurse Kaci Hickox, Boyfriend Plan to Leave Maine Town*, CNN (Nov. 10, 2014, 11:30 AM), http://www.cnn.com/2014/11/09/health/ebola-nurse/ [http://perma.cc/4C5X-TGNM].

[217] *Id.*

[218] *Id.*

[219] *See* PONEMON INST. LLC, *supra* note 31, at 1 (according to the Ponemon Institute study, a compromised file could cost a company up to $200).