5-1-2014

Maximizing The Future: The Case For Mandating Fraud Prevention Tools In Electronic Health Record Software

Ryan Potente

MAXIMIZING THE FUTURE: THE CASE FOR MANDATING FRAUD PREVENTION TOOLS IN ELECTRONIC HEALTH RECORD SOFTWARE

RYAN POTENTE[1]

INTRODUCTION

For decades, the U.S. health care system has been plagued by inefficiencies that have contributed to the rising cost of health care.[2] In 2011, the federal government spent an astounding $2.7 trillion dollars on health care.[3] To put this figure in proper perspective, consider that, excluding the United States, only four countries in the entire world have a GDP that exceeds $2.7 trillion.[4] In an effort to curb health care spending, and also promote better quality of care, the United States has made the move towards electronic health records (hereinafter "EHRs").[5] There is little doubt that EHRs represent the future of health care in the United States, but if that future is going to be bright, the federal government has to ensure that EHR systems do exacerbate the problem of health care fraud. [6]

---

[1] Seton Hall University School of Law, J.D. Candidate 2013.

[2] According to the World Health Organization (WHO), the U.S. spent more on health care per capita, $7,146, and more on health care as percentage of its GDP, 15.2%, than any other nation in 2008. World Health Organization, World Health Statistics: 2011, http://www.who.int/gho/publications/world_health_statistics/EN_WHS2011_Full.pdf

[3] *See* Centers for Medicare and Medicaid Services, National Health Expenditure Projections 2011-2021, https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/Proj2011PDF.pdf.

[4] Trading Economics, Gross Domestic Product (GDP), List by Country, http://www.tradingeconomics.com/gdp-list-by-country.

[5] The American Recovery and Reinvestment Act of 2009 (Recovery Act) authorizes the Centers for Medicare and Medicaid Services (CMS) to award incentive payments for health care professionals who demonstrate 'meaningful use' of 'certified' EHR systems. In 2015, financial penalties are schedule to take effect for Medicare and Medicaid providers who do not transition to EHRs. *See* 42 C.F.R. 495.6l; 42 C.F.R 495; 42 C.F.R 102.

[6] Healthcare fraud is defined generally as an "intentional deception or misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or the entity or to some other party." National Health Care Anti-fraud Association. What is Healthcare Fraud?, www.nhcaa.org/about_health_care_fraud/Consumer_Information

EHR systems include certain timesaving software tools, such as copy and paste functions, that increase the efficiency of health care delivery. However, these very same software tools can be also be used to commit fraud faster and with greater ease than ever before.[7] Unfortunately, the federal government and ONC[8] have largely ignored this vexing issue.[9] This point is perhaps most apparent after consideration of the "certification regulations," which were adopted by the ONC in 2010 and set forth the required minimum capabilities of an EHR system. Despite setting forth extensive functional requirements, there is not even one provision in the regulations that is specifically designed to prevent fraud.[10] This paper will argue that, in order to avoid an increase in health care fraud, the certification regulations must be amended to include functional

---

[7] *See generally* Lisa Eramo. Stopping Fraud: Detecting and Preventing Fraud in the e-Health Era. Journal of AHIMA, March 2011, American Health Information Management Association, http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048698.hcsp?dDocName=bok1_048698.

[8] The ONC, Office of the National Coordinator for Health Information Technology, is organizationally located within the Office of HHS and "is the principal Federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information." About ONC: The Office of the National Coordinator, HealthIT, May 5, 2012,http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__onc/1200.

[9] Since 2009, the Obama Administration has held dozens of public meetings on electronic health record policies and standards, but none that focused primarily on fraud control. Fred Schulte, Billing Software Helps Medical Professionals Document Higher Fees, The Center for Public Integrity, September 19, 2012, http://www.publicintegrity.org/2012/09/19/10812/growth-electronic-medical-records-eases-path-inflated-bills. *See also* Donald Simborg, There is No Neutral Position on Fraud, Journal of the American Informatics Association, July, 2011 (discussing specific examples of how the leadership at the ONC has chosen not to be proactive with regard to fraud management.)

[10] "To date, federal meaningful use requirements do not include a fraud prevention component, and EHR certification related to the program thus does not require it." *Id*. *See also* 45 C.F.R 170.302, 304,306 and 314 (hereinafter "the certification regulations provisions.") It is important to note that the certification regulations do contain some provisions that are helpful towards deterring fraud. For example, 45 C.F.R. 170.302(o) requires each EHR system to "assign a unique name/and or tracking number for identifying and tracking user identity." However, anything in the regulations helpful to preventing fraud is "limited to those which overlap with security and privacy concerns which motivated their inclusion." Simborg, *supra* note 9. This paper takes the position that the certification regulations must include provisions that are *specifically tailored* to the unique threats of fraud created by the use of EHR software tools in order to avoid an increase in health care fraud.

requirements that are specifically tailored to address the unique fraud threats caused by EHR systems (these functional requirements will hereinafter be referred to as "fraud prevention software tools.")

This paper is organized as follows: Part I discusses how EHR software can be used to increase the ease and speed of committing health care fraud, and presents data that suggests fraud has already increased as a result of unprotected EHR systems.[11] Part II sets forth four policy reasons why this problem should be addressed in the certification regulations with fraud prevention software tools. Part III recommends specifics fraud prevention tools that should be included in the certification regulations. Finally, Part IV concludes this paper by addressing some likely criticisms to use of fraud software tools.

I. UNSECURED EHR SYSTEMS INCREASE THE EASE & SPEED OF COMMITTING HEALTH CARE FRAUD

In a recent New York Times article, Dr. David J. Brailer, former National Coordinator of the ONC, stated unequivocally the use of EHRs "makes it faster and easier to be fraudulent."[12] Dr. Brailer's sentiment is hardly ground breaking. In fact, two separate reports commissioned by the federal government have reached the same conclusion.[13] EHR systems increase the ease and speed of committing health care fraud primarily because they include software tools that make it exceedingly easy to create a

[11] Healthcare fraud is defined as an "intentional deception or misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or the entity or to some other party." National Health Care Anti-fraud Association. What is Healthcare Fraud?, www.nhcaa.org/about_health_care_fraud/Consumer_Information.

[12] Reed Albeson, Medicare Bills Rise as Records Turn Electronics, N.Y. Times, Sept. 21 2012.

[13] "Without a deliberate effort to build fraud management into [electronic systems], healthcare payers and consumers will be exposed to new and potentially increased vulnerability to electronically enabled healthcare fraud." Foundation of Research and Education of AHIMA, Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities, 13, September 30, 2005. *See* also, discussed extensively in Part III, RTI International, Recommended Requirements for Enhancing Data Quality in Electronic Health Records, May 2007, http://www.rti.org/pubs/enhancing_data_quality_in_ehrs.pdf.

false record of what occurred during a medical encounter. Most commonly, the false record will be used to *deliberately* 'bill for a service not rendered' or provide the basis for 'upcoding.'[14] These schemes already represent the two most popular forms of health care fraud[15], and as such, any increase in their occurrence through the exploitation of EHR software is a grave concern.

A few of the most frequently abused EHR tools include: (i) one-click notes, (ii) copy and paste features, and (iii) billing decision message prompts (hereinafter "message prompts.) Although one-click notes and copy and paste features function differently, they largely present the same problem in that they both increase the speed and ease of inserting false information into a medical record. One-click notes, as the name suggests,

[14] 'Billing for services not rendered' is a scheme wherein a bill is deliberately submitted for payment even though no medical service was actually provided. 'Upcoding,' in contrast, is a scheme wherein the health care providers submits a bill using a procedure code that yields a higher payment than the code for the service that was truly rendered. Federal Bureau of Investigation, Financial Crimes Report to the Public: 2010-2011, http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011. It is important to distinguish these two schemes, which are committed deliberately, with inadvertent errors in coding for which, according to the Wall Street Journal, "there are no comprehensive statistics." Jessica Silver-Greenberg, How to Fight a Bogus Bill, The Wall Street Journal, February 18, 2011. The paper's focus is on those whom deliberately abuse EHR software tools to commit healthcare fraud faster and with greater ease.

[15] The specific percentage of fraud attributable to these activities vary from study to study, but all indicate upcoding and billing for services not rendered account for the majority of health care fraud. Foundation of Research and Education of AHIMA, Automated Coding Software: Development and Use to Enhance Anti-Fraud Activities, July, 2005, Page 8. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031700.pdf (hereinafter "AHIMA coding report.") The AHIMA coding report concluded these schemes account for 77% of fraud, 43% for upcoding and 34% for billing for services not rendered. *Id.* In contrast, DataWatch, utilizing data from public and private payers, determined these schemes accounted for 56% of fraud, 22% for upcoding and 34% for billing for services not rendered. Datawatch, Health Insurance Fraud Busters, Business and Health, 2000, pg. 18.

allow physicians to paste a pre-programmed examination note with just one-click.[16] For example, some systems allow the following to be entered into an EHR with just one-click: "[t]he chest expansion is normal and symmetrical. There is no dullness to percussion. Both diaphragms move adequately. There are no rales, rhonchi, wheezes, egophony nor whispered pectoriloquy."[17] Some systems go even further, and allow physicians to create longer and more detailed notes that could cover extremely intricate examinations.[18]

Whereas one-click notes are typically limited to certain common procedures, the potential for abuse of copy and paste features is almost limitless. A common scheme involves pasting the same examination findings for multiple patients, a practice known as cloning.[19] However, cut and paste features can be abused even more subtlety when it is limited to the same patient's record. For example, consider a situation where a patient is hospitalized with an infection and the standard of care requires the patient be examined thoroughly each day to gauge the progress of treatment. By using the copy and paste feature, a physician can make it appear that the initial examination, which may have been very thorough and therefore entitled to a high billing code, was completed every day. However, in actuality, a much shorter examination was most likely completed after the initial examination. Anecdotal evidence suggests this type of fraud is exceedingly

[16] Daniel Essin, The Ethical Dilemma Created by EHRs, Physicians Practice, June 18, 2012, http://www.physicianspractice.com/blog/content/article/1462168/2083374

[17] Donald Simborg, Promoting Electronic Health Record Adoption: Is It the Correct Focus?, Journal of the American Medical Informatics Association, 2008, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2274790.

[18] *Id.* For example, Medical Training Billing Corp. (MTBC), a web-based EHR company, offers an EHR system, ChartsPro™, that includes one-click notes that encompass entire exams "for musculoskeletal, vascular, and lymphatic systems." Medical Training Billing Corp., EHR Features, 2012, http://www.mtbc.com/ehr-features.aspx.

[19] Albeson, *supra* note 12.

common. For example, Robert E. Hirschtick, M.D., Associate Professor at Northwestern Medical School, noted that after EHR software was adopted at Northwestern "virtually all of [the examination] notes are longer, recombinant versions of previous notes… Ideally, old information and diagnostic impressions are deleted and new ones added. In reality, however, there is no deletion, only additions." [20]

Message prompts also contribute to the creation of false documentation in EHRs, but in a very different way than one-click notes or cut and paste features. In general, message prompts help physicians select the medical billing code that corresponds with the service provided and, in turn, determines the amount of reimbursement.[21] While coding assistance is fine in and of itself, many prompts go too far and actively increase the ease of committing health care fraud by specifically advising physicians what documentation is required to justify higher billing codes.[22] Typically, message prompts notify the physician if the billing code he or she entered is not justified by the current EHR documentation, and then advises how to reach the higher code. [23] However, some EHR

[20] Robert Hirschtick, Copy and Paste, JAMA, 2006, http://courses.washington.edu/hmed665i/copyandpaste.pdf

[21] Rich Henriksen, Healthcare Coding, Billing & Reimbursement Overview, Healthcare Consulting, http://minneanalytics.org/files/Rich_Henriksen.pdf.

[22] While it could be argued that prompts do not increase the ease of committing fraud, since physicians intuitively know documentation for a more serious diagnosis carries a higher reimbursement, it should be emphasized that the delineations between billing codes can be extremely minute and are notoriously difficult to understand. There are currently 17,000 different diagnosis codes and that number will increase to 144,000 when the ICD-10 billing requirements take effect on October 1, 2014. Jennifer Bresnick, Q&A: ICD-10 Progress With Pat Schmitter, EHRIntelligence, November 7, 2012, http://ehrintelligence.com/2012/11/07/qa-icd-10-progress-with-pat-schmitter. The use of prompts after that time will be extremely important to all physicians, whether they desire to upcode or not, since "ICD-10 will inherently bring to need for more specific documentation." Lee Ford, Coding & Clinical Documentation Challenges of ICD-10, North Carolina Health Information Management Assoc., June 24, 2010, www.nchima.org/smart05-bin/public/downloadlibrary?&itemid2307.

[23] Mildred L. Johnson, Electronic Medical Records Playbook, Texas Tech University Health Science Center Office of Billing Compliance, June 5, 2008, http://www.ttuhsc.edu/elpaso/it/documents/EMR_Playbook.pdf.

systems go even further and indicate how to reach higher codes even when the initial code entered by the physician *was justified* by the EHR documentation. [24]

Recent data suggests the potentialities of fraud discussed above have been realized in the areas of the country that have already adopted EHR systems. In September of 2012, the New York Times conducted a data analysis of Medicare claims that revealed hospitals with EHR systems are increasing their use of the highest billing codes.[25] A particularly egregious example is Baptist Hospital in Nashville, Tennessee which submitted 82% of its claims at the highest level in the year after it adopted an EHR system. [26] Over all, hospitals that received government incentives to adopt EHRs showed a 47% rise in Medicare payments at higher levels from 2006 to 2010, compared to just a 32% rise in hospitals that have not received government incentives.[27] The Times' findings were confirmed by the Center of Public Integrity (CPI) which conducted a similar data analysis of claims from 2001 to 2010. [28] The CPI found, "thousands of providers turned to more expensive billing codes…despite little evidence that Medicare patients as a whole are older or sicker than in past years."[29] While no one cause could be identified, CPI concluded, "higher billing rates appear to be associated with the use of

[24] *Id.* Farzad Mostashari, the current National Coordinator for ONC, has recognized that prompts that suggest more documentation to reach a higher billing code "might be over the line." Robert Lowes, Federal EHR Office to Look at Overbilling Allegations, Medscape Medical News, October 19, 2012, http://www.medscape.com/viewarticle/772944.
[25] Albeson, s*upra* note 12.
[26] *Id.*
[27] *Id.*
[28] Fred Schulte, Center Investigation Suggests Costs From Upcoding and Other Abuses Likely Top $11 Billion, Center for Public Integrity, September 15, 2012, http://publicintegrity.org/2012/09/15/10810/how-doctors-and-hospitals-have-collected-billions-questionable-medicare-fees.
[29] *Id.*

medical records and billing software... which make it easy to create detailed patient files with just a few mouse clicks."[30]

While the initial data is admittedly limited, it has gotten the attention of the federal government. In a letter dated September 24, 2012, the Secretary of HHS Kathleen Sebelius and U.S. Attorney General Eric Holder advised the chief executive officers of five leading hospital associations that there are "troubling indications" that some providers are using EHRs to "game the system." [31] The letter reiterated the government's commitment to catching fraudsters noting, "law enforcement will take appropriate steps to pursue health care providers who misused electronic health records."[32] While the letter serves as a strong warning, immediate federal action is required if the government hopes to slow down fraud attributable to EHRs. For the policy reasons set forth in Part II, below, federal action should take the form of amending the certification regulations to require all EHR systems include fraud prevention software tools.

II. POLICY ARGUMENTS THAT SUPPORT AMENDING THE CERTIFICATION REGULATIONS TO REQUIRE FRAUD PREVENTION TOOLS IN EHRS

Before setting forth the policy reasons why the certification regulations should be amended, it is important to note that there is little doubt that the ONC has the statutory authority to make the changes this paper will advocate. Under 42 U.S.C.A 300jj-11(c)(5), the ONC is given the responsibility to "keep or recognize a program for the voluntary certification of health information technology."[33] Moreover, the ONC is given broad

[30] *Id.*
[31] Letter from Obama Administration on Billing, September 24, 2012, http://www.nytimes.com/ /interactive/2012/09/25/business/25medicare-doc.html?ref=business.
[32] *Id.*
[33] The HHS news release announcing that the ONC had issued a final rule for EHR certification explicitly cites to this statutory section. "This final rule is issued under the authority provided to

discretion in determining the underlying certification criteria under 42 U.S.C.A. 300jj-14(b)(3) which states the ONC "shall adopt…implementation specifications and certification criteria as necessary." Further, ONC leadership has previously recognized, through its words and official actions, that it has the ability to mandate fraud prevention tools in EHR systems. [34]

There are at least four policy arguments that support amending the federal certification regulations to mandate the inclusion of fraud prevention tools in EHRs. First, given the tremendous negative impact of fraud and abuse on the U.S health care system, a strong federal response is required to prevent further damage from the exploitation of EHR software. Second, the responsive tactics currently emphasized by the government are of limited effectiveness in combating health care fraud, and as such, more emphasis must be placed on proactive fraud prevention tactics like EHR fraud prevention tools. Third, data mining, the government's primary proactive fraud prevention approach, cannot slow significantly slow down the increased fraud due to use of EHR software tools, and therefore, should be supplemented with more and diversified proactive approaches. Fourth, and finally, fraud prevention tools should be included in all EHRs

---

the National Coordinator for Health Information Technology in section 3001(c)(5) of the Public Health Service Act (PHSA) as added by the HITECH Act." HHS, ONC Issues Final Rule to Establish Certification Program for Electronic Health Record Technology, June 18, 2010, http://www.hhs.gov/news/press/2010pres/06/20100618d.html.

[34] Dr. Simborg notes that shortly after the creation of the ONC it's first National Coordinator, Dr. David Brailer, convened a panel of health law experts and posed to them the question, should the ONC "be neutral with regard to fraud or proactive in combating fraud?" *See* Simborg, *supra* note 9. Further, the ONC subsequently commissioned a report prepared by RTI International whose sole purpose was to propose fraud prevention software tools. While RTI's suggestions were not adopted, its clear the ONC believed it had the ability to adopt such recommendations and further, none of the public comments received in response to the report questioned the ONC's ability to adopt the recommendations. RTI International, Recommended Requirements for Enhancing Data Quality in Electronic Health Records. May 2007, http://www.rti.org/pubs/ehcancing_data_quality_in_ehrs.pdf. This report will be discussed extensively in Part III of this paper.

because not only will they ensure EHRs are not used to increase fraud, but if adequately designed, they can actively decrease all health care fraud.

A. POLICY ARGUMENT 1: GIVEN THE TREMENDOUS NEGATIVE IMPACT OF FRAUD AND ABUSE ON THE HEALTH CARE SYSTEM, A STRONG FEDERAL RESPONSE IS REQUIRED TO PREVENT FURTHER DAMAGE FROM THE EXPLOITATION OF EHR SOFTWARE.

Dr. Donald W. Simborg, the chairman of several federal panels that examined the potential for fraud in electronic health systems, compared fraud and abuse in the health care system to "doping and bicycling…[e]verybody knows it's going on."[35] The statistics concerning the extent of fraud and abuse in the U.S. health care system can only be described as simply staggering. According to a 2008 study by the Association of Certified Fraud Examiners, (1) about $133 billion of all payments by CMS were distributed improperly due to the filing of illegitimate claims, (2) $50 billion in payments made by Blue Cross and Blue Shield were for fraudulent payments, and (3) $100 billion in other private or patient payments were for some form of improper billing.[36] Based upon this conservative figure, $283 billion, the amount lost due to fraud and abuse in the U.S. each year towers over the GDP of Ireland, $218 billion. [37]

It is important to emphasize that health care fraud is not a victimless crime. The pervasiveness of fraud and abuse in the system contributes to the rising cost of health care, which places increased financial burdens on patients and employers alike.[38] For

---

[35] Albeson, *supra* note 12.

[36] Jeffrey Helton, Avoiding Fraud Risks Associated with EHRs, Health Financial Management Association, July 2010, http://www.mfrpc.com/Default.aspx?DN=f927c939-4f17-44ae-870d-dcbaa978d59c.

[37] Trading Economics, Ireland GDP, http://www.tradingeconomics.com/ireland/gdp.

[38] In 2006, the National Coalition on Health Care (NCHC) noted that "inappropriate care, waste and fraud" were major contributors to the rising cost of medical care and health insurance in the U.S. National Coalition on Health Care (NCHC). Health Insurance Cost: Facts on the Cost of Health Care. 2007, http://www.nchc.org/facts/costs.html.

patients, this means having to pay higher insurance premiums, which many families are unable to do during the current economic recession.[39] For employers, health care fraud increases the overall cost of doing business, and in some instances, has resulted in employers dropping insurance coverage altogether.[40] Given this information, it is not surprising the National Health Care Anti-Fraud Association (NHCAA) has opined "[f]or many Americans, the increased expense resulting from fraud could mean the difference between making health insurance a reality or not."[41]

While increased health care costs are troublesome, what's more disconcerting is that fraud and abuse can directly and adversely affect patient care for those who are already insured. [42] For example, consider a situation where a diagnostic note is included in a patient's EHR solely to justify the use of a higher billing code. At first glance, the erroneous note appears to have no direct impact on the patient's health. After all, the patient has already received care and is presumably on the road to recovery. However, it is important to remember that the erroneous note will remain in the patient's EHR and, as such, could adversely affect future clinical decisions.[43] Dr. Hirschtick, whose

---

[39] National Health Care Anti-Fraud Association, The Problem of Health Care Fraud, http://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-problem-of-health-care-fraud.aspx. Unsurprisingly, lack of medical insurance directly impacts the health of patients. A study by Harvard University linked the lack of insurance to 45,000 death per year in the U.S. Reed Abelson, Harvard Medical Study Links Lack of Insurance to 45,000 U.S. Death a Year, N.Y. Times, September 17, 2009, http://prescriptions.blogs.nytimes.com/2009/09/17/harvard-medical-study-links-lack-of-insurance-to-45000-us-deaths-a-year.

[40] *Id.*

[41] *Id.*

[42] Unfortunately, there are numerous concrete examples of patients being harmed as a result of health care fraud and abuse. One of the more egregious cases involves a Chicago cardiologist that performed over seven hundred and fifty medically unnecessary heart catherizations over a 10-year fraud scheme that resulted in at least two deaths. The physician was eventually sentenced to federal prison in 2002. Bruce Japsen, Edgewater Doctor's Sentence is 12 Years, Chicago Tribune, June 29, 2002, http://articles.chicagotribune.com/2002-06-29/business/020629.

[43] In Money and Outpatient Psychiatry: Practice Guidelines from Accounts to Ethics, Cecilia M. Mikalac contends that the inclusion of a false diagnosis in a patient's medical record can cause

experiences with copying and pasting in EHRs were discussed in Part I, provides perspective on how easily a physician could be misled by an erroneous note. "The patient does seem fully coherent now, but the EMR says she's demented and who are you going to believe, EMR or a demented patient?...everything in the EMR becomes true." [44]

Patient care can be affected by fraud and abuse in even more subtle ways. For example, fraud and abuse can decrease the finite health insurance benefits available to already insured patients. [45] Patients who have private health insurance often have lifetime caps or other limits on benefits under their policies. Every time a claim is falsely paid in a patient's name, the dollar amount counts toward that patient's lifetime or other limits. [46] This means that when a patient legitimately needs his or her insurance benefits the most, they may have already been exhausted. [47]

Given the tremendous impact of fraud on the health care system, a strong federal response is required to prevent further damage from the exploitation of EHR software. This paper advocates for the strongest conceivable federal response to this burgeoning problem by calling for amendments to the certifications regulations that will change the minimum requirements for each and every EHR system in the U.S. It is important to emphasize that this growing problem should be addressed through federal action since

---

societal harm as well by distorting the prevalence of certain diseases. She notes, "distorting diagnoses makes it difficult for governments and insurers to obtain accurate information for calculating current and future health care costs and skews statistics …about the prevalence of psychiatric illness." Cecilia M. Mikalac, Money and Outpatient Psychiatry: Practice Guidelines from Accounts to Ethics, pg, 58, New York: W.W. Norton, 2005.

[44] Dr. Hirschtick, *supra* note 15.

[45] The Affordable Care Act (ACA) eliminates all annual and lifetime limits on health insurance benefits starting in 2014. *See* 42 U.S.C.A. § 300gg-11.

[46] NCHC, *supra* note 38.

[47] *Id.*

health care fraud is truly a national problem.[48] This is especially true with respect to upcoding, which as discussed previously, is one of primary types of fraud that is increased when EHR software is exploited. In September of 2012, CPI released a report that found physicians have billed Medicare at progressively higher rates over the past decade and concluded "a significant portion of the added charges are likely due to 'upcoding.'"[49] CPI's investigation revealed that the increased upcoding was among "thousands of doctors, from *a broad range of specialties and locales*."[50] Consistent with this assertion, when U.S. counties were ranked by percentage of claims submitted at the highest billing codes, the report found the 20 most aggressive coding counties were disbursed among 13 different states.[51]

The government's response to this vexing problem must not only be strong, but it must be immediate as well. According to HHS estimates, the use of EHR systems will increase dramatically over the next few years. By 2015, 85% of hospitals will use EHR systems, as opposed to just 35% this year. Further, the use of EHRs by independent physicians is estimated to increase by approximately 25% within just the next year. [52] The government must seize this opportunity to adequately secure EHR software through amendments to the certification regulations before the amount of fraud attributable to EHR software explodes even further.

---

[48] Senator Chuck Grassley (R-IA), in discussing OIG's experience with fraud in the Medicaid program has noted, "it is perfectly clear from [OIG's] narratives that fraud and abuse in the Medicaid program is not concentrated in any specific area. Rather, it is widespread throughout the entire program." U.S. Senate Committee on Finance, Grassley Urges More Attention to Medicaid Fraud, August 18, 2004, http://www.finance.senate.gov/newsroom/chairman/release/?id=d0ca4434-add2-4213-92d9-9592925e931b.

[49] Schulte, *supra* note 27.

[50] *Id.*

[51] *Id.*

[52] HHS, Physicians Using EHR Technology, Express Positive Reviews, July 17, 2012, http://www.hhs.gov/news/press/2012pres/07/20120717a.html.

B. POLICY ARGUMENT 2: THE RESPONSIVE TACTICS CURRENTLY EMPHASIZED BY THE GOVERNMENT ARE OF LIMITED EFFECTIVENESS IN COMBATING HEALTH CARE FRAUD, AND AS SUCH, THE FEDERAL GOVERNMENT MUST PLACE MORE EMPHASIZE ON PROACTIVE TACTICS, SUCH AS EHR FRAUD PREVENTION SOFTWARE TOOLS, TO CURB THE EXPLOITATION OF EHR SOFTWARE.

Cesare Beccaria[53] once famously wrote, "it is better to prevent crimes than to punish them. This is the fundamental principle of good legislation."[54] The reasoning behind Beccaria's statement is quite obvious and inherently logical. It is always preferable to avoid the negative consequences of bad behavior, if possible, than to hope to effectively deal with them after the fact.[55] Curiously, the federal government has largely ignored preventative measures in its fight against health care fraud, even though, it has relied heavily upon them to avoid other great harms to the country.[56] Given the undeniable failure of the government's responsive tactics in fighting health care fraud, and upcoding in particular, the federal government must shift its focus towards more proactive measures, such as fraud prevention software tools, to curb the exploitation of EHR systems.

---

[53] Cesare Beccaria is a 18th century Italian philosopher whose writings, particularly *On Crimes and Punishment*, formed the basis for many modern criminology theories. Dr. Cecil E. Greek, Criminological Theory: Cesare Beccaria, Florida State University, November 22, 2005, http://www.criminology.fsu.edu/crimtheory/beccaria.htm.

[54] Cesare Beccaria, On Crimes and Punishment, 1785, http://www.constitution.org/cb/crim_pun41.txt.

[55] "Most criminologists agree that it is far better to prevent crime in the first place than to allow it to happen and then invoke a criminal justice response to it." Quint Thurman, Community Policing, Cincinnati, OH: Anderson Pub., 1997.

[56] The most notable example would be the government's approach to fighting terrorism. The USA Patriot Act provides law enforcement officers with tremendous latitude in surveying and detaining individuals in an effort to prevent acts of terrorism. Clearly, the U.S. government has made a concerted effort to prevent terrorism, as opposed to effectively dealing with the devastating consequences of terrorism after the fact. Likewise, in recognition of the tremendous harm caused by health care fraud, the government must place more emphasis on preventative measures.

Historically, the U.S. government has emphasized responsive approaches, such as post payment data-analysis, to identify fraud after the fact, and aggressive litigation to deter other dishonest health care providers from committing fraud.[57] The government's responsive tactics have proven to be of limited effectiveness. Studies indicate that only a tiny portion of health care fraud is identified through responsive tactics. A report prepared by the American Health Information Management Association (AHIMA) estimated that only three to ten percent of healthcare fraud is ever identified.[58] William J. Rudman, PhD, a co-author of the AHIMA report, asserted, "we are probably only at the tip of the iceberg in terms of being able to identify…fraud."[59] Further, it takes years to discover the small portion of fraud that is actually uncovered through responsive tactics. Dr. Rudman noted that instances of fraud that are detected "only surface after years of aberrant data patterns raise a red flag." [60] It can take years to identify fraud through responsive tactics even when a medical institution reviews its **own records**. According to Dr. Rudman, "in big corporations, it may take four or five years to document cases of fraud."[61]

When the government identifies fraud, severe financial penalties are typically levied against those who have abused the system. [62] The government loves to publicize

---

[57] Dr. Simborg has opined "[w]hat we do now is pay and chase. You pay the bill and then do a pattern analysis to find outliers. Then a sting operation to recover maybe a million or billion dollars…This is a drop in the bucket. We are talking about a $250 billion problem." Eramo, *supra* note 7.

[58] Foundation of Research and Education of AHIMA. A Study of Health Care Fraud and Abuse: Implications for Professionals Managing Health Information. Nov, 2010. Page 2. http://ahimafoundation.org/downloads/pdfs/Fraud%20and%20Abuse%20-%20final%2011-4-10.pdf.

[59] Eramo, *supra* note 7.

[60] *Id.*

[61] *Id.*

[62] A Department of Justice (DOJ) news release indicates the government obtained over $3 billion dollars in judgments and settlements in health care fraud and abuse cases in 2011. United States

the large amounts that have been recovered through fraud and abuse litigation,[63] however, the amounts recovered pale in comparison to the financial damage done to the system. According to a Department of Justice (DOJ) press release, the federal government recovered $3 billion dollars in 2011 from judgments and settlements resulting from health care fraud investigations.[64] While this figure is impressive in isolation, consider that $5 billion is stolen from the system as a result of health care fraud **every week**. [65]

While responsive tactics are generally ineffective in fighting all types of health care fraud, as the above figures demonstrate, they have proven particularly inept at counteracting upcoding and billing for services not rendered. Of the $3 billion recovered by the DOJ in 2011, the vast majority, $2.2 billion, came from improvident pharmaceutical companies.[66] Therefore, comparatively little was recovered from health care professionals that commit health care fraud through upcoding and billing for services not rendered.[67] What's more, studies suggests that the small amount recovered from upcoding physicians each year is almost entirely attributable to whistleblowers coming forward rather than the federal government's responsive investigative techniques. PCI's

---

DOJ, Justice Department Recovers $3 Billion in False Claims Act Cases in Fiscal Year 2011, December 19, 2011, http://www.justice.gov/opa/pr/2011/December/11-civ-1665.html (hereafter "DOJ press release.")

[63] There are no shortage of the examples of the government publicizing its large fraud and abuse monetary recoveries. The latest and most notable example came during the first Presidential debate of 2012 when President Obama proudly proclaimed, "we went after medical fraud in Medicare and Medicaid very aggressively, more aggressively than ever before, and have saved tens of billions of dollars, $50 billion of waste taken out of the system." Presidential Debate Questions and Transcript (October 3, 2012), http://www.politico.com/news/stories/1012/81991_Page4.html#ixzz29qJmqHrw.

[64] DOJ press release, *supra* note 62.

[65] It is estimated health care fraud results in $283 billion lost each year. This number, $283 billion, divided by the amount of weeks in a year, 52, results in an average of $5.4 billion stolen each week as a result of health care fraud. Helton, *supra* note 36.

[66] DOJ press release, *supra* note 62.

[67] This is significant since health care professionals commit 72% of all health care fraud. Thomas D. Musco, et. al., Health Insurers' Anti-Fraud Programs, Health Insurance Association of America, 1999, http://www.claim.org/workshops_separate/00FC07.pdf.

September 2012 report, discussed above, specifically asserted the government "typically has no way of find out [about persistent upcoding] unless someone on the inside comes forward and alerts them." [68] If responsive tactics cannot effectively curb upcoding and billing for services not rendered in general, there is absolutely no reason to believe such tactics will address the increased instances of these types of fraud that will result from the exploitation of EHR software.

C. POLICY ARGUMENT 3: DATA MINING, THE PRIMARY PROACTIVE APPROACH BEING UTILIZED BY THE GOVERNMENT, CANNOT SIGNIFICANTLY SLOW FRAUD AND ABUSE BY ITSELF, AND THEREFORE, OTHER PROACTIVE APPROACHES MUST BE IMPLEMENTED.

Over the past few years, fraud prevention, as opposed to paying and chasing, has gained some traction in the federal government.[69] Undoubtedly, data mining is the center piece of the government's initial shift toward more proactive fraud tactics. [70] Data mining is a pattern discovery process that relies upon large volumes of data to infer meaningful patterns and relationships between data items.[71] Roughly stated, the purpose of data

---

[68] Schulte, *supra* note 47.

[69] HHS Secretary Kathleen Sebelius stated on March 15, 2011, during the joint HHS / DOJ Detroit Fraud Prevention Summit, that HHS is moving away from the "old pay and chase model." Detroit Fraud Prevention Summit, HHS, March 15, 2011, http://www.hhs.gov/secretary/about/speeches/sp20110315.html.

[70] Robert Radick, a Forbes Magazine contributor, has noted that the use of data mining has become the "bread and butter" of the federal government's fight against health care fraud. Robert Radick, Claims Data and Health Care Fraud: The Controversy Continues, Forbes, September 25, 2012, http://www.forbes.com/sites/insider/2012/09/25/claims-data-and-health-care-fraud-the-controversy-continues. Two recent developments are noteworthy. In 2011, the federal government passed regulations that allow State Medicaid Fraud Control Units (MCFUs) to seek federal funds to start data mining Medicaid claims. *See* CFR 1007.19(e)(2). In an even more aggressive approach, the government recently began to use revamped data-mining technology to predict and identify potentially fraudulent Medicare claims to help stop fraudulent claims before they are paid. Fierce HealthIT, New Technology To Help Fight Medicare Fraud, June 22, 2011, http://www.fiercehealthit.com/press-releases/new-technology-help-fight-medicare-fraud.

[71] Guisseppi A. Forgionne et. al., An Intelligent Data Mining System to Detect Health Care Fraud, page 152, January 1, 2000, http://www.igi-global.com/chapter/intelligent-data-mining-system-detect/9223.

mining is to extract useful information from data using complex algorithms.[72] In the health care context, the goal of data mining is to significantly decrease health care fraud by uncovering fraudulent billing practices. However, there are several factors that suggest the government is unlikely to obtain far reaching success with data mining as its sole proactive approach.[73]

First, as a preliminary matter, it is important to note that data mining is a relatively new developed methodology and technology, coming into prominence only in 1994.[74] As such, some suggest there is a lack of published well-researched methods and algorithms in any context, let alone the complex health care environment, for this approach to be successful over the long term.[75] Even if the most beneficial algorithms are currently in place, the government is not guaranteed long-term success with this approach since any data mining initiative must continually adapt to changing circumstances to remain successful. [76] As time goes by, fraudsters will change their behaviors in response to the current algorithms.[77] Tom Fawcett, a respected data mining scholar, has noted "[w]ithin the near future after uncovering the current modus operandi of professional fraudsters,

---

[72] Frank Cohen, Data Mining As An Audit Tool, Health Care Finance News, July 6, 2011, http://www.healthcarefinancenews.com/blog/data-mining-audit-tool.

[73] Louis Saccoccio, CEO of National Health Care Anti-Fraud Association, recently testified before Congress and advocated strongly for a diversified approach to fraud prevention. "Health care fraud takes many forms and is a serious problem regardless of the mode of health care delivery. Similarly, anti-fraud efforts must be multi-faceted, as there is no single solution to this problem." Statement of Louis Saccoccio before U.S. House of Representatives, Energy and Commerce Committee, November 28, 2012, http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/Health/20121128/HHRG-112-IF14-WState-SaccoccioL-20121128.pdf.

[74] Gerald Tan et. al., Data Mining Applications in Health Care, Journal of Health Information Management, http://www.himss.org/content/files/jhim/19-2/datamining.pdf.

[75] Clifton Phua, A Comprehensive Survey of Data-Mining Fraud Detection Research. Artificial Intelligence Review, 2005, http://arxiv.org/ftp/arxiv/papers/1009/1009.6119.pdf.

[76] *Id.*

[77] *Id.*

these same fraudsters will continually supply new or modified styles of fraud until the detection systems start generating false negatives again." [78]

Even assuming the government adequately deals with this issue, there are still serious doubts as to whether there is reliable medical data to analyze. Medicaid claims data in particular has come under intense scrutiny, and high-ranking governmental officials have recognized the unreliability of such data. For example, in June of this year, HHS Regional Inspector General Ann Maxwell recently acknowledged to the House Committee on Oversight and Government Reform that much of the Medicaid data that is mined and analyzed to identify overpayments and fraud is not "current, available, complete, [or] accurate." [79] Regional Inspector General Maxwell concluded, "[t]he poor quality of the Medicaid data…hindered their ability to efficiently detect suspicious trends in Medicaid claims for further auditing or investigation." [80]

The initial data suggests that data mining is not having as significant of an impact as originally hoped. In 2011, federal regulations were passed that permit State Medicaid Fraud Control Units (MCFUs) to seek federal funds to start data mining.[81] Florida's MCFU was the first state entity to obtain federal funding.[82] In its first 8 months of

[78] *Id.*
[79] Assessing Medicare and Medicaid Program Integrity, Testimony of: Ann Maxwell Regional Inspector General Office of Inspector General (OIG) of HSS, June 7, 2002, https://oig.hhs.gov/testimony/docs/2012/Maxwell_testimony_06072012%20.pdf.
[80] *Id.*
[81] *See* CFR 1007.19(e)(2).
[82] HHS, HHS Announces New Tool to Help Fight Health Care Fraud in Florida, July 15, 2010, http://www.hhs.gov/news/press/2010pres/07/20100715a.html.

utilizing data mining technology, the state's efforts only resulted in 2 court cases and 18 complaints opened. [83]

Perhaps it is too early to pass judgment on Florida's efforts, but even in more established data mining programs, the results are far from over whelming. For example, consider the Medicare-Medicaid Data Match Program (frequently referred to as the "Medi-Medi Project.") The Medi-Medi project combines Medicare and Medicaid claims and then utilizes computer algorithms to search for payment anomalies.[84] The program started in 2001 in California, and has slowly expanded to other portions of the country. [85] In 2007, when the program was in operation in 10 states, the Chief Financial Officer of CMS at the time, Timothy B. Hill, asserted, "to date…$15 million in overpayments have been referred for collection, and $25 million in improper payments have been denied before payment was made."[86] The paltry amounts recovered, in comparison to the billion stolen each year, suggest the federal government should utilize a more diversified approach that includes different types of proactive tactics, such as fraud prevention software tools, in order to address the increase of fraud through exploitation of EHR systems.

D. POLICY ARGUMENT 4: FRAUD PREVENTION SOFTWARE TOOLS SHOULD BE REQUIRED IN ALL EHRS BECAUSE THEY CAN NOT ONLY ADDRESS THE PROBLEM OF INCREASED FRAUD DUE TO ABUSE OF EHR TOOLS, THEY CAN DECREASE ALL HEALTH CARE FRAUD.

[83] Florida Agency for Health Care Administration Medicaid Fraud Control Unit Department of Legal Affairs, The State's Efforts to Control Medicaid Fraud and Abuse FY 2010-2011. Page 9, http://ahca.myfloria.com/Executive/Inspector_General/docs.
2010_11_Fraud_and_Abuse_Annual_Report.pdf.
[84] Kathy Giannangelo, Mining Medicare and Medicaid Data to Detect Fraud, Journal of AHIMA, July 2007, http://library.ahima.org/xpedio/groups/public/docuents/ahima/bok1_034462.
[85] *Id.*
[86] Statement of Timothy B. Hill, Chief Financial Officer (CMS) on Medicare Program Integrity before Committee on Ways and Means, U.S. House of Representatives, March 8, 2007, http://www.hhs.gov/asl/testify/2007/03/t20070308g.html.

Health care fraud is not a homogenous crime. It is committed by a number of different perpetrators whom utilize varied fraudulent schemes.[87] Therefore, admittedly, the problem is unlikely to be completely eliminated by any singular proactive approach. However, fraud prevention software tools could become the strongest tool in combating health care fraud because they can not only prevent abuse of EHR tools, but, if properly designed, they can also help decrease all instances of health care fraud.

Studies indicate health care professionals commit the majority of health care fraud, 72%,[88] and that this fraud is most commonly perpetrated through either upcoding or billing for services not rendered.[89] As noted in Part I, EHR software includes several timesaving tools that increase the speed and ease of committing these specific types of fraud. Fraud prevention tools could be designed to make sure these tools are not abused. However, there is no reason why fraud tools have to be limited to ensuring EHR features do not increase the problem of upcoding and billing for services not rendered in the electronic setting. If properly designed, EHR software could help eliminate these problems altogether.

A simple example helps demonstrate this point. To address the problem of billing for services not rendered, EHRs could require advanced identity authentication at the point of care, such as a biometric thumbprint scan, to ensure a medical examination has actually taken place. [90] This requirement would ensure that EHR tools, such as one-click

[87] While health care fraud commonly involves doctors billing for services not rendered or upcoding, non-health care providers commit nearly 30% of fraud each year. Musco, *supra* note 67.
[88] *Id.*
[89] AHIMA coding report, *supra* note 15.
[90] Eramo, *supra* note 7. This fraud prevention software tool is examined further in Part III.

notes, cannot be used to help create a false record that can then be used to bill for services not rendered. However, this requirement would not only ensure that EHR software tools are not abused, it would also actively decrease all instances of this type of fraud. If a unique thumbprint is required, health care professionals cannot create a record for a visit out of thin air regardless of whether they would have used EHR software tools to increase the speed and ease of doing so. As the above example demonstrates, EHR software is sufficiently malleable to transform it from a tool that increases fraud to a tool that actively deters it.

III. FRAUD PREVENTION SOFTWARE TOOL RECOMMENDATIONS

In 2007, RTI International published a report entitled Recommended Requirements for Enhancing Data Quality in Electronic Health Records. [91] The report's primary focus was to identify requirements for EHR systems that would "prevent fraud from occurring, as well as detect fraud both prospectively and retrospectively."[92] The report set forth fourteen distinct functional requirements.[93] While the ONC commissioned the report, its functional requirements were framed as non-binding "recommendations to

[91] RTI International, *supra* note 13.
[92] *Id.* at ES-2.
[93] RTI's recommendations are grouped into the following fourteen distinct functional requirements: (1) audit functions and features, (2) provider identification, (3) user access authorization, (4) documentation process issues, (5) evaluation and management (E&M) coding, (6) proxy authorship, (7) record modification after signature, (8) auditor access to patient record, (9) EHR traceability, (10) patient involvement in anti-fraud, (11) patient identity-proofing, (12) structured and coded data, (13) integrity of EHR transmission, and (14) accurate linkage of claims to clinical records. Id. at 4-1. Each of the aforementioned requirements has several distinct parts and therefore, it is probably more accurate to state RTI recommended over 60 EHR systems requirements. *Id*. at 4-6 to 4-17.

the industry"[94] and subsequently ignored when the certification regulations were passed.[95]

Fraud prevention tools hold tremendous promise and should be required in all EHR systems. However, these tools must be designed with an eye towards the risks associated with EHR systems if they are going to be effective. As noted, the abuse of EHR software leads to increased instances of upcoding and billing for services not rendered. Therefore, the certifications regulations must include several tools that are specifically designed to prevent these types of fraud. However, the regulations must also consider the effect each tool will have on the delivery of care because, while fraud is a tremendous problem, the majority of physicians do not commit health care fraud. [96] The certification regulations must strike a delicate balance. The government did not encourage the adoption of EHR's for its own sake, but rather with hopes of promoting a system that is more efficient in all facets, including the delivery of care.[97] Therefore, fraud prevention tools must be specifically designed to prevent fraud without stripping EHR systems of the timesaving capabilities that made them appealing in the first place.

Below, this paper recommends three fraud prevention tools that were initially advocated by RTI in its 2007 report. The first two recommendations, the regulation of message prompts and use of biometric identification, are specifically designed to prevent upcoding and billing for services not rendered. The third recommendation, which increases the auditing capability of payers, is designed to prevent the payment of

[94] *Id*. at ES-2.
[95] *See generally* Eramo, *supra* note 7. The certification regulation provisions, *supra* note 7.
[96] The NHCAA has opined "[t]he majority of health care fraud is committed by a very small minority of dishonest health care providers." NHCAA, *supra* note 39.
[97] "Electronic health record systems are the key to the transformation of healthcare…widespread use has the potential to improve the quality of care, increase patient safety, reduce medical errors, and control health care costs." *Id*. at ES-1.

fraudulent claims should other fraud prevention tools not prevent the creation of a false record. Although these recommendations vary greatly in their approach, they all have the benefit of not impeding the timesaving tools that make EHR software beneficial to the majority of physicians who do not abuse the system. The certification regulations should be immediately amended so that these fraud prevention tools are required in all EHR systems.

A. RECOMMENDATION 1: THE CERTIFICATION REGULATIONS SHOULD REQUIRE ALL EHRS HAVE MESSAGE PROMPTS THAT: (1) ADVISE A PHYSICIAN IF THE SELECTED BILLING CODE IS INCONSISTENT WITH THE ENCOUNTER NOTE DOCUMENTATION, AND (2) DO NOT SUGGEST WHAT ADDITIONAL DOCUMENTATION IS REQUIRED TO UTILIZE A HIGHER BILLING CODE.

RTI's fifth functional requirement addressed message prompts in EHR software. RTI recommended that all EHR systems should prompt a physician when the billing code entered is inconsistent with the documentation in the encounter notes.[98] Further, RTI recommended that EHR software not suggest what documentation is required to reach a higher billing code.[99] These interrelated requirements should be included in the regulations because they address the problem of upcoding head on.

Some studies suggest upcoding accounts for nearly half of all health care fraud, [100] and as previously discussed, the exploitation of EHR software tools leads to an increase in this type of fraud. As such, the certifications regulations must include fraud prevention tools that curb this activity. Each part of this recommendation aggressively addresses the problem of upcoding. First, explicitly advising physicians when a billing code is inconsistent with note documentation prevents upcoding by simultaneously deterring

[98] RTI International, *supra* note 13 at 4-11.
[99] *Id*.
[100] AHIMA coding report, *supra* note 15.

fraudsters[101] intending to upcode and educating honest physicians on proper billing practices to avoid unintentional upcoding. The prompt serves as a strong deterrent because fraudsters are immediately be put on notice that their billing practices are questionable and likely to alert the attention of the authorities. Further, all physicians would attain a tremendous educational benefit from the prompts because it would provide physicians with immediate feedback concerning their coding practices.[102]

Second, message prompts should not suggest how to reach higher billing codes to ensure that EHR software does not actively entice upcoding.[103] Going forward, the certification regulations must be developed with an eye towards the fact that software developers have a strong incentive to include tools that make it exceedingly easy to upcode.[104] In order to prosper, software developers must demonstrate to physicians that their products will result in a return on investment. To do so, software companies have pitched physicians on the ability of their products to increase income through the use of

---

[101] The prompt would serve as an even greater deterrent to upcoding if it prevented the physician from submitting the claim at all when an inconsistent code is entered. This drastic approach could be entertained if more measured tactics do not slow the upcoding epidemic.

[102] Physicians have consistently sought clarification from CMS concerning proper coding practices. In a letter addressed to HHS and the DOJ, the Association of Academic Health Centers (AAHC) noted "clarification of evaluation and management services coding has been a priority for AAHC, and we are ready and willing to with (CMS) and our members to address this issue." AAHC Responds to HHS and DOJ Letter; Calls for Clarification on Guidance, September 25, 2012, http://www.aahcdc.org/Policy/PressReleases/PRView/ArticleId/112/AAHC-RESPONDS-TO-HHS-AND-DOJ-LETTER-CALLS-FOR-CLARIFICATION-ON-GUIDANCE.aspx

[103] It is particularly important that EHR software does not entice physicians to upcode since physicians already have such a strong financial incentive to do so. Studies show that "raising the [billing] code by a single level on two patients a day can increase a doctor's income by more than $15,000 over the course of a year and is not likely to raise suspicions." Fred Schulte, Judgment Calls on Billing Make 'Upcoding' Prosecutions Rare, The Center for Public Integrity, September 15, 2012, http://www.publicintegrity.org/2012/09/15/10835/judgment-calls-billing-make-upcoding-prosecutions-rare.

physicians commit fraud. The AHIMA noted, "there is unintended incentive for fraud because…software developers need to prove a return on investment for the coding products. This issue must be considered in fraud prevention activities." AHIMA coding report, *supra* note 15 at pg. 22.

higher codes.[105] Ross Kopel, a sociology professor at the University of Pennsylvania, observed that EHR software sales agents stress how the machines help doctors document the work they do, but "everybody knows there is a wink, wink behind that [with an underlying understanding that software] will help … make the patient's visit look more involved than it is…[and] generate additional revenue."[106] In recognition of the strong financial incentive software developers have to develop easily abused software, it is imperative that the certification regulations prohibit tools, such as higher billing code prompts, that entice physicians to upcode.

B. RECOMMENDATION 2: THE CERTIFICATION REGULATIONS SHOULD REQUIRE ADVANCED PATIENT IDENTITY AUTHENTICATION AT THE POINT OF CARE BEFORE PERMITTING A PHYSICIAN TO ENTER AN EXAMINATION NOTE.

Regulating EHR message prompts, in the ways discussed above, would create a strong deterrent to upcoding. To adequately address the other primary type of fraud increased through the exploitation of EHRs, billing for services not rendered, the certification regulations must place a heavy burden on providers to demonstrate a medical encounter has actually occurred. This can be accomplished by requiring that EHR systems identify patients through the use of a biometric thumb scan at the point of care.[107]

In order to prevent all billing for services not rendered, EHR software should do more than simply record that a patient's identity has been verified, as was suggested by

---

[105] EHR software companies make it clear that the use of higher coding levels could help physicians obtain a small fortune. For example, one manufacturer predicts a rise of one coding level for each patient visit, which it said could add up to $225,000 over the course of a year. Another cites a medical journal report that notes a medical practice in Utah produced an average billable gain of $26 per patient visit. Schulte, *supra* note 9.

[106] *Id.*

[107] Eramo, *supra* note 7; Ken Congdon, Are Biometrics the Key to Health IT Security?, Healthcare Technology Online, May 20, 2010, http://www.heatlhcaretechnologyonline.com/doc.mvc/Are-Biometrics-The-Key-To-Health-IT-Security-0001.

RTI in its report. [108] Instead, the software should go further and require advanced identity authentication before allowing the physician to take any action, such as enter an examination note. By requiring identity authentication first, all instances of billing for services not rendered would be decreased, as explained in Part II.D, and importantly, none of the EHR time-savings tools would be impaired. As noted above, it is important that the certification regulations adopt requirements that can combat fraud, and at the same time, do not hinder the tools that make the provision of care more efficient through use of EHRs. This requirement does not hamper any of the EHRs timesaving tools, and could actually make the entire physician office experience more efficient. As explained by Ken Congdon:[109]

> After an initial scan, the identifying characteristics in the scan can be linked to the patient's record. In every subsequent visit, the patient will no longer have to go through the lengthy registration process (i.e. filling out paper work, submitting an insurance card, etc.). Instead, all of this data can be automatically populated based on the stored information linked to the biometric scan.[110]

In addition to curbing billing for services not rendered, this requirement would also help eliminate medical identity theft, one of the fastest growing types of health care fraud.[111] Medical identity theft most commonly occurs when a person uses someone

[108] RTI's eleventh functional requirement, patient-identity proofing, suggested EHRs systems be able to "document/record that identity-proofing was completed and the method used to verify." RTI International, *supra* note 13 at 4-14.
[109] Mr. Congdon is the Editor-in-Chief of Healthcare Technology Online.
[110] Congdon, *supra* note 107.
[111] RTI, *supra* note 13 at 4-14. A 2011 study conducted by the Ponemon Institute estimated the annual economic impact of medical identity theft to be $30.9 billion. Ponemon Institute, Second Annual Survey on Medical Identity Theft, Page 1, March 2011, https://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/1_types%20of%20fraud_medical%20study.PDF

else's medical record to obtain medical goods or services.[112] In 2010, 1.42 million Americans were the victims of medical identity theft. [113] In addition to defrauding payers, medical identity theft can adversely affect patient care. "When a victim's records are merged with a thief using the same identity… that record becomes 'polluted,' and the victim may be…misdiagnosed based on this inaccurate information."[114] According to a 2011 report conducted by the Ponemon Institute, 15% of medical identity theft ultimately results in either mistreatment or misdiagnosis of illness.[115]

While there is little doubt that biometric identification can be a powerful fraud prevention tool, the use of biometrics raises privacy concerns for many.[116] Privacy advocates express particular concern over the consequences that could result from the unauthorized distribution of such sensitive information. Chris Dunn, associate legal director at the New York Civil Liberties Union, has opined "anytime you surrender private information like DNA, fingerprints, iris scans or palm prints, you need to understand that the information can be stored in a database, distributed to the world and used in ways you never intended."[117] However, those in the biometrics industry contend such views are misguided and the product of media depictions of biometrics that "do not

---

[112] Rick Kam, A Glimpse Inside the $234 Billion World of Medical Fraud, Government HealthIT, http://www.govhealthit.com/news/glimpse-inside-234-billion-world-medical-id-theft.

[113] Ponemon, *supra* note 111.

[114] Kam, *supra* note 112.

[115] Ponemon, *supra* note 111 at pg. 8.

[116] According to a survey conducted by the Citizen and Immigration Canada (CIC), 48% of respondents expressed privacy concerns over the use biometric technology. Andrew Patrick, Societal Aspects of Biometrics, Institute for Information Technology, February 1, 2003, http://zing.ncsl.nist.gov/biousa/docs/bcc/BCC%20Societal%20Aspects%20of%20Biometrics%20v06.pdf.

[117] Kathleen Lucadamo, NYU Hospital Scans Palms to Track Patients Without IDs, NY Daily News, July 25, 2011, http://articles.nydailynews.com/2011-07-25/local/29831318_1_patient-safety-palm-scans.

accurately depict biometric technology, and leave [viewers] with ill conceived perceptions about the technology actually works."[118]

A review of how biometric technology identifies patients confirms that privacy concerns are largely unwarranted.[119] When a patient's thumb is initially scanned by a biometric device, the patient's biometric data is instantly converted into an otherwise unrelated data-string.[120] It is this data-string, and not an image of the patient's thumbprint, that is retained and used to verify the patient's identity. In fact, since the patient's thumbprint is instantly converted, a physical image of the patient's fingerprint is *never stored or transmitted* across a network. [121] Furthermore, "it is nearly impossible to reverse engineer the [data-string] and successfully 'steal' [or re-create a patient's] biometric identity." [122] Even assuming the data string could be reversed engineered to re-create an image of the patient's thumbprint, the image would most likely be useless to a potential identity thief since most biometric systems do not associates data-strings with

---

[118] Jeff Carter, Misinformation About Biometric Technology Continues to Fuel Functionality Misconceptions, M2SYS Biometric Technology, November 19, 2010, http://blog.m2sys.com/comments-on-recent-biometric-news-stories/misinformation-about-biometric-technology-continues-to-fuel-functionality-misconceptions. Data suggests the public as a whole does not have a true understanding of how biometric technology actually works. In fact, a survey conducted by the CIC found that 90% of respondents didn't even know what the term 'biometrics' meant. Patrick, *supra* note 116.

[119] Some contend that biometric identification actually increases medical privacy. "If biometrics make the data more secure, then you are actually doing more to protect people's privacy." Argus Global, Do Biometrics Breach Your Privacy?, August 20, 2012, http://www.biometricidentitymanagement.com/blog/do-biometrics-breach-your-privacy.

[120] Carter, *supra* note 119.

[121] *Id.*

[122] *Id. See also* Paige Backman, Biometric Identification and Privacy Concerns, Aird & Berlis, LLP, October 13, 2009, http://www.airdberlis.com/Templates/Articles/articleFiles/584/Biometric%20Identification%20and%20Privacy%20Concerns.pdf ("the original biometric data cannot be created from the stored information.")

patient names.[123] As the above discussion makes clear, biometric technology has advanced to a point where the chance of unauthorized distribution of biometric data has been all but eliminated. As such, privacy concerns should not prevent the implementation of biometric identification in all EHR systems.

C. RECOMMENDATION 3: THE CERTIFICATION REGULATIONS SHOULD PERMIT PAYERS TO HAVE READ-ONLY ACCESS TO A PATIENT'S ENTIRE EPISODE OF CARE.

RTI's eighth functional requirement addressed the auditing capabilities of EHRs.[124] RTI recommended that EHR systems allow payers read-only access to a patient's entire episode of care, as opposed to only each individual visit.[125] This recommendation should be included in the certification regulations because it will increase the information available to payers, and therefore, increase their ability to detect fraud as soon as possible after payment is made or, ideally, before payment is made.

Payers need adequate information in order to detect fraud. In its report, RTI noted that it is exceedingly difficult to detect fraud before payment is made due to the scant amount of information typically available to payers. "Detection of a fraudulent claim is often difficult when a payer has access only to EHR information for a single encounter."[126] As RTI notes, it is quite logical that "[r]eviewing information over an entire episode of care for a single patient [would result in] greater ability to detect fraud."[127] In recognition of the tremendous amount of damage being done by health care

[123] "9.9 times out of 10 biometric systems do not associate names with a biometric template so how would the criminal/hacker know who's biometric information it actually is?" Carter, *supra* note 119.

[124] RTI International, *supra* note 13 at 4-12.
[125] *Id*.
[126] *Id*.
[127] *Id*.

fraud, the regulations must allow for those in the best position to prevent fraud to have ample information to detect it.

While the hope is that software fraud tools will prevent the exploitation of EHR software tools, it will be admittedly difficult to craft tools to combat every single way the software can exploited. This requirement recognizes this fact and adds another layer of protection by giving payers a real chance to prevent fraudulent payments, and the many harms that flow there from. Beyond preventing payment of fraudulent claims, this requirement has the added benefit of not impeding delivery of care. The goal is to implement software protections that combat fraud without negatively impacting the majority of care that is unaffected by health care fraud. This requirement undoubtedly furthers this goal.

While this requirement has obvious advantages, it was controversial to privacy advocates.[128] Deborah Peel, head of the Patient Privacy Rights Foundation, when asked about this requirement opined, "[it] proposes to violate every American's health privacy to detect health care fraud." [129] The privacy concerns associated with this requirement are overstated and should not prevent its inclusion in the certification regulations.

There is no doubt that privacy is an issue that is important to many patients, [130] and should be an important consideration in shaping EHR fraud prevention tools. This requirement represents a measured approach that respects patient privacy. First, it must

---

[128] *See* generally Joseph Conn, Vendors, Privacy Actvisits Speak Out on Report, Modern Healthcare, August 24, 2007, http://www.modernhealthcare.com/article/20070824/INFO/308240 01/1029/FREE.

[129] *Id.*

[130] In a Gallup survey commissioned by the Institute for Health Freedom, 78% of sampled adults said it was very important that their medical records be kept confidential. The Gallup Organization, Public Attitudes Towards Medical Privacy, Page 2, September 2000, http://www.forhealthfreedom.org/Gallupsurvey/IHF-Gallup.pdf.

be emphasized that this requirement only grants payers access to information they have *already viewed*. By allowing payers access to an entire episode of care, the payer is in reality simply reviewing prior related bills for consistency. As such, this requirement makes it quicker and easier for the payer to detect fraud, yet, does not require patients to reveal new additional information in the process.

Further, this requirement represents a truly measured approach in that it limits payer access to identifiable episodes of care, and therefore, specifically excludes access to the patient's entire EHR. In many instances, payers will receive the same exact information that they normally would. For example, if the patient's current visit is unrelated to any prior medical issues or visits, such as a visit related to the seasonal flu, that singular visit constitutes the entire episode of care and, as such, the payer only receives information pertaining to that visit. This requirement does not attempt to "violate every American's health privacy" as Ms. Peel suggests. It simply asks patients to give up just a slither of privacy to help protect a system on the brink. The benefits of this requirement fair outweigh any privacy concerns and, as such, should be included in the certification regulations.

IV. CRITICISMS TO FRAUD PREVENTION SOFTWARE TOOLS

Although RTI's specific software tool recommendations were not adopted, the public comments to their report indicated strong public support for the proposal of fighting fraud by securing EHR software.[131] Those critical of RTI's report primarily focused upon concerns that arose from RTI's specific recommendations, and not the

[131] RTI International, *supra* note 13, at 4.2 ("The comments supplied indicate general support for combating fraud in electronic HIE systems.") In fact, the majority of responses received during the public comments period supported each recommendation made by RTI. *Id.*

general approach of fraud prevention software tools.[132] That being said, it is likely that the federal government and civil liberty groups will oppose the use of fraud software tools, albeit for very different reasons.

It is foreseeable that some in the Obama Administration will oppose fighting fraud through the use of software tools for fear of physician backlash. By all accounts, RTI's 2007 proposal was "totally ignored for fear of a physician backlash."[133] Dr. Robert Kolodner, a physician who headed the federal push for EHRs in 2007, acknowledged that fraud prevention took a backseat to steps likely to entice the medical community to embrace the new technology.[134]

The possibility of physician backlash is no longer a viable reason for the federal government to delay implementation of aggressive fraud prevention tools in EHRs. While enticing physicians to adopt EHR software is a laudable goal, it must be remembered that EHR adoption is not the ultimate goal.[135] If the amount of fraud in the system explodes due to use of EHR software, the desired goals of EHR adoption, mainly a more efficient and cost-effective health care system, may never be realized. Further, the government has already put in place policies that should sufficiently entice EHR adoption. Under the American Recovery and Reinvestment Act of 2009 (Recovery Act), physicians can receive significant financial payments if they display meaningful use of EHRs. [136] Further, the incentive to adopt EHR technology will increase tremendously in 2015 when

---

[132] Criticisms to the specific fraud tools recommended by this paper were addressed in Part III.
[133] Schulte, *supra* note 9.
[134] *Id.*
[135] "[The] goal is not adoption alone but 'meaningful use' of EHRs — that is, their use by providers to achieve significant improvements in care." David Blumenthal, The "Meaningful Use" Regulation for Electronic Health Records, The New England Journal of Medicine, August 5, 2010, http://www.nejm.org/doi/full/10.1056/NEJMp1006114.
[136] Physicians can receive a maximum of $44,000 through the Medicare Incentive Program, 42 C.F.R. 495.102, or $63,750 through the Medicaid Incentive Program, 42 C.F.R. 493.310.

the government will start penalizing those that do not utilize EHRs. [137] The excuses of the past must be abandoned so that the full benefits of EHRs can be realized.

In addition to opposition from the government, it also likely fraud prevention tools will arise concerns in civil liberties advocates. Fraud software tools represent an aggressive preventative approach to combating the exploitation of EHR systems. In recent years, there has been a public outcry against overly aggressive preventative policing measures. Specifically, there have been a number of demonstrations protesting what have been dubbed "preemptive law enforcement measures," wherein the government uses available information to predict who will commit certain offenses and then aggressively intervenes to prevent the commission of a crime.[138] A commonly used, and often criticized, preemptive law enforcement measure is "stop and frisk" which essentially permits law enforcement officers to detain and search anyone they consider suspicious.[139] Advocates argue "preemptive law enforcement [is] not only an oxymoron, but…[it] violates a number of civil rights."[140] Such measures are usually opposed on the

[137] For physicians who cannot demonstrate "meaningful use" by the 2015 deadline, Medicare reimbursements will be reduced by 1%. The deduction rate increases in subsequent years by 2% in 2016, 3% in 2017, 4% in 2018, and up to 95% depending on future adjustments. *See* 42 C.F.R. 495.102(b); 42 C.F.R. 495.310(a); Electronic Medical Records Deadline: Will I Be Assessed Penalties For Not Using An EMR System? Medical Records, http://www.medicalrecords.com/physicians/electronic-medical-records-deadline.

[138] *See generally* Michael Ratner, "The Meaning and Importance of Dissent," Hell No: Your Right to Dissent in 21st Century America, New York, NY:The New Press, 2011, 19-25.

[139] Robert Stolarik, Stop and Frisk Policy- New York City Police Department, NY Times, October 12, 2012, http://topics.nytimes.com/top/reference/timestopics/s/stop_and_frisk/index.html. While police officers must have a "reasonable suspicion" to engage in stop and frisks, New York City's own records indicate police officers typically rely on vague grounds such as "furtive" movements. *Id.*

[140] Paul Rexton Kan, "Law Enforcement and High Intensity Crime," Cartels at War, Washington D.C.: Potomac, 2012, 90.

grounds they violate the Fourth Amendment's guarantee of freedom from unreasonable searches and seizures.[141]

Preemptive law enforcement critics raise valid concerns, however, these concerns should not prevent adoption of the proposal set forth in this paper since fraud prevention software tools do not represent a truly preemptive law enforcement measure. Preemptive law enforcement involves measures, such as "stop and frisk," that involve either the detainment of an individual, or at the very least, some sort of actual police intervention, including surveillance, prior to the commission of a crime. Fraud prevention tools, in contrast, simply add protections to EHRs so they are not used to commit illegal ends. Fraud software tools do not involve police intervention or surveillance, quite to the contrary, these measures seek to remove the need of law enforcement by making it impossible to misuse EHR software tools. As such, fraud prevention tools raise no constitutional concerns. Since, as the above discussion demonstrates, the concerns associated with fraud prevention software are largely unwarranted, the certification regulations should be amended to mandate their inclusion in all EHR systems.

CONCLUSION

The federal government has taken bold steps to ensure that EHRs are a focal part of the U.S. health care system. EHRs promise better patient care, increased efficiency, and reduced health care costs. In short, EHRs may hold the key to a brighter future for U.S. health care. However, the same features of EHRs that engender hope, also cast a dark ominous shadow on the future. EHR software tools increase the speed of health care delivery, yet also provide dishonest health care professionals with almost endless

[141] Stolarik, *supra* note 139.

opportunities to game the system and increase the widespread damage caused by health care fraud.

To protect the future of the U.S. health care system, the federal government must amend the certification regulations to mandate the inclusion of fraud prevention tools in EHR software. Fraud prevention tools will not only ensure that EHRs do not increase the amount of fraud in the system, but if designed properly, they can significantly eliminate all instances of health care fraud. The fraud tools should strive to address upcoding and billing for services not rendered, which account for the vast majority of health care fraud, and are the types of fraud most likely to increase through the exploitation of EHR systems. Requiring identity authentication at the point of care and putting strong controls on message prompts, recommended in Part III of this paper, would go along way in preventing these problems. Conversely, permitting payers read only access to a patient's entire episode of care would go along way in detecting these problems if dishonest health care professionals somehow find a wrinkle in the system. With immediate and appropriate action, the future with EHRs is still bright.