CONNECTICUT
LAW REVIEW

VOLUME 47 MAY 2015 NUMBER 4

Note

Reading Between the Lines of Electronic Health Records: The Health Information Technology for Economic and Clinical Health Act and Its Implications for Health Care Fraud and Information Security

JOSEPH D. SZEREJKO

The Health Information Technology for Economic and Clinical Health (HITECH) Act, which Congress passed as part of the American Recovery and Reinvestment Act of 2009, has set in motion a widespread increase in the use of electronic health records (EHRs) across the American health care industry. While EHRs are not new to health care, their being the standard format for purposes of documenting patients' health records across the United States is a modern reality. By monetarily rewarding health care providers for adopting and using EHRs and by penalizing noncompliant providers, the HITECH Act seeks to achieve this reality through its meaningful use incentive program.

This Note examines the ways in which widespread use of EHRs in the American health care industry will impact the security and privacy of protected health information. Furthermore, this Note predicts how the proliferation of EHRs may complicate, and in some cases obstruct, health care fraud detection. In this vein, this Note assesses the tactical options available to anti-fraud authorities as they adapt their auditing, detection, and enforcement efforts to an electronic world. Finally, this Note offers recommendations as to how prosecutors, law enforcement authorities, lawmakers, providers, and patients can improve health care fraud detection.

NOTE CONTENTS

Reading Between the Lines of Electronic Health Records: The Health Information Technology for Economic and Clinical Health Act and Its Implications for Health Care Fraud and Information Security

JOSEPH D. SZEREJKO*

I. INTRODUCTION

It is an understatement to say that technology has influenced health care's development over the past several decades. For example, diabetes patients can monitor their insulin levels with a transdermal patch,[1] radiologists in India can read an American patient's X-rays at the click of a mouse,[2] and surgeons can operate on patients with robots.[3] Technology constantly improves the quality of health care and medical research, but it also influences the law. Accordingly, legal practitioners, legislators, and health care providers should monitor technological health care developments every step of the way, for they have rippling effects.

The proliferation of electronic health records (EHRs)[4] is a major trend in health information technology[5] that has impacted—and will continue to

---

* J.D. Candidate, University of Connecticut School of Law, Class of 2015. I would like to thank everyone at the United States Attorney's Office in Hartford for providing me with valuable insight and guidance with respect to prosecuting health care fraud. Further, I would like to thank Special Assistant United States Attorney Michael Ahern and Michael Cohen, Inspector at the United States Department of Health and Human Services for sparking my interest in the issues encompassed in this Note. I would also like to thank Adjunct Professor Joshua Stein from the University of Connecticut School of Law for sharing his thoughts with me on the privacy and security of EHRs. I would also like to thank my friends and family for supporting me throughout my writing this Note. Finally, I would especially like to thank the editors of Volumes 46 and 47 of the *Connecticut Law Review* for their help in preparing my Note for publication. This Note would not have been possible without their valuable efforts and recommendations.

[1] *See, e.g.*, *What is V-Go?*, V-GO, https://www.go-vgo.com/what-is-vgo (last visited Jan. 28, 2015) (describing a transdermal patch that monitors and delivers insulin for diabetes patients).

[2] *See, e.g.*, James Brice, *Globalization Comes to Radiology: Global Nighthawks Thrive While Outsourcers Hire Foreign-Trained Radiologists to Read for U.S. Imaging Practices*, DIAGNOSTIC IMAGING.COM (Nov. 2003), http://web.mit.edu/outsourcing/class1/DI-radiology-1.htm (describing a doctor's routine practice of performing radiological diagnoses in Bangalore, India for patients in Atlanta, Georgia).

[3] *See, e.g.*, *The Da Vinci Surgical System*, INTUITIVE SURGICAL, http://www.intuitivesurgical.com /products/davinci_surgical_system/ (last visited Jan. 28, 2015) (describing the da Vinci surgical robot, a pioneering piece of machinery in the field of robotic surgery).

[4] The legislative, medical, legal, and academic materials discussing this topic occasionally refer to these records as electronic medical records (EMRs). This Note will refer to them as EHRs.

[5] *See* David Blumenthal, *Launching HITECH*, 362 NEW ENG. J. MED. 382, 382 (2010) (describing how installation and use of EHRs is an integral part of using health information technology).

impact—the intertwined medical and legal fields in the twenty-first century. EHRs streamline the provision of health care, make patients' care more comprehensive, and put providers on equal footing from an informational perspective.[6] For instance, if paramedics in Los Angeles roll an unconscious vacationing New Yorker into Cedars-Sinai's Emergency Room after he has suffered a stroke, EHR technology permits attending ER physicians—after having looked at the patient's identification—to look up the patient's medical history and other personal health information at the click of a mouse.[7] On the other hand, a hospital employee with bad intentions can access an EHR database and use patients' confidential proprietary information for theft and other criminal purposes.[8] Therein lies the rub: great technological innovations that facilitate saving lives also provide criminals with tools for their respective trade.

EHR technology enhances the speed and efficacy of medicine and many providers have integrated EHR systems into their practices for these very reasons. However, while the federal government is able to cite a plethora of practical justifications for implementing a nationwide EHR system, there is also cause for concern. There are various reasons why many providers have not yet implemented EHR technology into their business models, but the primary reason that abstaining providers articulate is that implementation is too costly.[9] In the first decade of the twenty-first century, health care providers in the United States, particularly smaller, private physician practices, were reluctant to launch EHR databases for

---

[6] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-481, ELECTRONIC HEALTH RECORDS: FIRST YEAR OF CMS'S INCENTIVE PROGRAMS SHOWS OPPORTUNITIES TO IMPROVE PROCESSES TO VERIFY PROVIDERS MET REQUIREMENTS 1 (2012) ("EHRs can be used . . . to electronically collect, store, retrieve, and transfer clinical information related to patients' care, allowing ready access to this information by multiple providers in different locations"); *but see* Spencer S. Jones et al., *Electronic Health Record Adoption and Quality Improvement in U.S. Hospitals*, 16 AM. J. MANAGED CARE SP 64, SP 64 (2010) (offering a key finding that U.S. hospitals' adoption of more advanced EHR systems actually was associated with decreases in quality improvement for treatment of heart patients).

[7] *See, e.g.*, Gregory A. Wilson et al., *The Effect of Immediate Access to a Computerized Medical Record on Physician Test Ordering: A Controlled Clinical Trial in the Emergency Room*, 72 AM. J. PUB. HEALTH 698, 702 (1982) (suggesting that the patients who benefit most from treating doctors' decision-making are those who have pre-existing medical records in computerized format at the time of treatment decisions).

[8] *See, e.g.*, Erica Meltzer, *Nurse Faces 51 Counts of Medical Records, ID Theft at Boulder Community Hospital*, COLORADODAILY.COM (Sept. 27, 2011, 5:16 PM), http://www.coloradodaily.com/ci_18989489?source=most_viewed#axzz1ZFlRjK2P (reporting the story of a nurse who, while working for a nurse staffing agency in the Denver metro area, improperly accessed over a hundred patient medical records and used identity information to purchase credit cards and make other purchases).

[9] *See* Michael McBride, *Measuring EHR Pain Points: High Cost, Poor Functionality Outweigh Benefits, Ease of Access*, MED. ECON. (Feb. 10, 2014), http://medicaleconomics.modernmedicine.com/medical-economics/content/tags/ehr/measuring-ehr-pain-points-high-cost-poor-functionality-outweigh-b?page=full (discussing how many physicians complain about the high costs associated with implementing and using EHRs).

their patient files.[10] In order to install and use EHR technology, providers must shoulder the substantial costs of maintenance, training, and support for EHR databases in addition to the costs of purchasing and installing them.[11] Providers' reluctance in implementing EHR technology seems more justifiable in this light. Nevertheless, the federal government and various state governments have started to tackle providers' reluctance in the interest of bringing the benefits of EHR technology to fruition.[12]

On February 17, 2009, as part of the American Recovery and Reinvestment Act of 2009,[13] Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[14] The ultimate goal of the HITECH Act is to induce health care providers across the nation to "meaningfully use" EHR technology for all of their patients' medical records.[15] Among other legislative objectives, the HITECH Act provides incentive payments to clinicians and hospitals that implement and "meaningfully use" EHR technology.[16] Further, the Act enforces standard EHR requirements and aims to incentivize nearly all covered health care entities to adopt EHR technology by 2019.[17] In essence, the Act's "meaningful use" program conditions clinicians' receipt of incentive payments on their employment of EHR technology in such a way that

---

[10] In 2006, the Healthcare Information Management Systems Society interviewed 2,500 physician offices around the United States and found that all of them had a practice management system. However, when the interviewers asked the offices if they had an EHR system, only 26% of them answered in the affirmative. Further, when the interviewers asked the other 74% of the offices if they planned on purchasing EHR technology in the next two years, the predominant answer was no. *Can Small Healthcare Groups Feasibly Adopt Electronic Medical Records Technology?: Hearing Before the Subcomm. on Regulatory Reform and Oversight of the H. Comm. on Small Bus.*, 109th Cong. 6 (2006) (statement of Jack Price, Healthcare Information and Management Systems Society, HIMSS Analytics).

[11] *Id.* at 7.

[12] *See* John Rancourt & Fadesola Adetosoye, *EHR Adoption Encouraged by State Meaningful Use Acceleration Challenge 2.0*, HEALTHIT BUZZ (Apr. 3, 2013, 5:25 PM), http://www.healthit.gov/buzz-blog/meaningful-use/ehr-adoption-encouraged-state-meaningful-acceleration-challenge-20/ ("Last year, ONC, the Centers for Medicare & Medicaid Services (CMS), and our partners in the states stepped on [the] gas pedal of Meaningful Use Acceleration—our catch-all phrase for all efforts related to bringing down costs and improving health care quality through EHR adoption and meeting Meaningful Use criteria.").

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

[14] Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.).

[15] David Blumenthal & Marilyn Tavenner, *The "Meaningful Use" Regulation for Electronic Health Records*, 363 NEW ENG. J. MED. 501, 501 (2010).

[16] Mark Faccenda & Lara Parkin, *Meaningful Use – What Does it Mean to You?*, 23 HEALTH LAW. 10, 10 (2011).

[17] *See Whitepaper: A Summary of the HITECH Act*, ATHENAHEALTH, INC. 2 (Mar. 2009), http://www.athenahealth.com/_doc/pdf/HITECH_Fact_Sheet_Whitepaper.pdf ("Prior to the HITECH Act, the Congressional Budget Office (CBO) anticipated that under existing laws, 65% of physicians would have adopted an EHR by 2019. It now estimates that the incentive mechanisms of the HITECH Act will boost these adoption rates to 90% of physicians.").

benefits their patients and health care in general.[18] Specifically, the HITECH Act makes as much as $27 billion in incentive payments available over ten years, and makes as much as $44,000 through Medicare and $63,750 through Medicaid available to each clinician.[19]

Some of the major difficulties that have already arisen—and that likely will become more pronounced—include: the widespread costs that clinicians have been forced to bear in preparing to comply with the mandate; the transformed availability of patients' protected health information in cyber media; and the difficulties that EHR technology will create for detecting health care fraud.[20] Other issues likely will arise as EHRs become increasingly prevalent.

The purpose of this Note is twofold. First, it seeks to evaluate several major impacts that the HITECH Act's EHR agenda will have on the privacy and security of protected health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[21] Second, this Note seeks to examine the difficulties that the proliferation of EHRs will create for prosecutors in detecting health care fraud and recommends how responsible authorities should respond to these difficulties. Part II begins with a description of the HITECH Act's EHR agenda, particularly with respect to its incentive payment program and its promulgation of meaningful use requirements. Further, Part II evaluates the HITECH Act's modifications to HIPAA, including its inclusion of business associates as liable entities[22] and its establishment of the data breach notification law.[23] Part III begins by discussing the False Claims Act[24] and federal criminal statutes that penalize health care fraud. It then assesses how the HITECH Act's meaningful use program, EHR incentive program, and its modifications to HIPAA will alter prosecutorial efforts to detect health care fraud. Part IV makes preliminary recommendations to prosecutors, legislators, and administrative officials regarding the difficulties that EHRs create for detecting health care fraud. This Note concludes by recognizing

---

[18] *See* Blumenthal & Tavenner, *supra* note 15, at 501–03 (discussing the meaningful use core and menu objectives and noting how they progressively encourage usage of EHRs to improve clinical outcomes).

[19] *Id.* at 501.

[20] *See* Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J.L. & TECH. 103, 119–24 (2008) (discussing the increases in potential for data errors, risk of security breach, and economic cost associated with integration of EHR systems).

[21] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C.); *see* 45 C.F.R. §§ 164.302–164.318 (2013) (providing the HIPAA Security Rule); 45 C.F.R. §§ 164.500–164.534 (2013) (providing the HIPAA Privacy Rule).

[22] 45 C.F.R. §§ 164.306(a)(1)–(4).

[23] 42 U.S.C. § 17932 (2012).

[24] False Claims Act, Pub. L. No. 111-21, 123 Stat. 1621 (1863) (codified as amended at 31 U.S.C. §§ 3729–3733 (2012)).

the substantial benefits of EHR technology and by making predictions about the future of EHRs under the current regulatory regime.

II. THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT AND THE SPREAD OF ELECTRONIC HEALTH RECORDS

A. *The Electronic Health Record Incentive Payment Program*

The HITECH Act's incentive payment program aims to promote the widespread use of EHR technology across the American health care industry by providing carrots for those professionals and hospitals that shoulder the onerous burdens associated with implementing and using this technology.[25] One of the primary means by which the HITECH Act achieves this overarching goal is its grant of permission to the Centers for Medicare and Medicaid Services to provide incentive payments to Medicare-eligible professionals, hospitals, and critical access hospitals[26] that "demonstrate meaningful use of certified EHR technology."[27] The HITECH Act also sets forth a similar Medicaid EHR incentive program.[28] The Centers for Medicare and Medicaid Services propound that the incentive program is not simply a reimbursement system for purchasing EHR technology, and they stress that payments are conditioned upon use.[29] Thus, these payments are spoils that must go to the victors—those Medicare- and Medicaid-eligible professionals, hospitals, and critical access hospitals that succeed in meeting the Act's EHR use requirements.

The HITECH Act also established the Office of the National Coordinator for Health Information Technology (National Coordinator),

---

[25] *See* Nitin Chhoda, *HITECH Act Explained*, EMR NEWS: DUMBED DOWN EMR (July 9, 2012), http://www.emrnews.com/the-hitech-act/ ("Most of the incentives focus on promoting the use of electronic medical records and electronic health records. Because electronic records cut down on long term costs, but require an initial investment that many clinics don't want to make, ARRA and the HITECH Act offer financial benefits if you make the switch.").

[26] The Social Security Act provides, *inter alia*, that a State may designate a health care facility as a critical access hospital if it is in a statutorily-defined rural area, is at least thirty-five miles away from any other hospital, makes 24-hour emergency care services available, and provides no more than twenty-five acute care inpatient beds. 42 U.S.C. § 1395i-4(c)(2)(B) (2012).

[27] *EHR Incentive Programs*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/EHRIncentivePrograms/ (last updated Apr. 2, 2015, 4:02 PM) [hereinafter *EHR Incentive Programs*].

[28] *Medicare and Medicaid EHR Incentive Program Basics*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Basics.html (last updated Feb. 18, 2015, 2:45 PM) [hereinafter *Medicare and Medicaid EHR Incentive Program Basics*]. The Medicare Incentive Program launched in 2011, so payments to participants who started then will continue annually until 2016. Participants can begin the program after 2011, at which point a participant's five-year continuous payment plan starts accumulating. However, the last year to begin is 2014. Participants who begin the program in 2014 will finish receiving incentive payments in 2019. *Id.*

[29] *EHR Incentive Programs*, *supra* note 27.

which is an office within the Department of Health and Human Services.[30] The National Coordinator is responsible for reviewing and endorsing the EHR meaningful use requirements promulgated by the Health Information Technology Standards Committee (Standards Committee),[31] coordinating health information technology efforts between Executive Branch departments and the Department of Health and Human Services, and updating the Federal Health IT Strategic Plan[32] to include specific benchmarks and metrics.[33] The Standards Committee's standards and certification specifications provide a basic framework that every EHR system should have, such that eligible professionals and hospitals using EHR technology have a reference point with which to compare their own EHR systems.[34] The HITECH Act also established the Health Information Technology Policy Committee (Policy Committee), which is primarily responsible for making policy recommendations to the National Coordinator regarding the policy issues surrounding EHR technology.[35]

---

[30] 42 U.S.C. § 300jj-11(a) (2012).

[31] This Committee, comprised of health care providers, researchers, technology vendors, purchasers, health plans, consumers, and health care employees, is primarily responsible for testing—with the assistance of other federal agencies such as the National Institute for Standards and Technology—certain standards and certification specifications for implementing coordinated EHR technology. Further, this Committee must ultimately recommend these standards to the National Coordinator. *See id.* § 300jj-13 (providing for the establishment, duties, membership, and operations of the Standards Committee).

[32] The National Coordinator released the Federal Health IT Strategic Plan in 2008 at the behest of President George W. Bush's 2004 Executive Order calling for the development and implementation of a more robust health information technology infrastructure in the U.S. From a general perspective, the 2008 Plan sought, *inter alia*, to encourage more widespread use of electronic health information and to make such use more coordinated amongst providers and patients, such that provision of care became more efficient and successful. *See The ONC-Coordinated Federal Health Information Technology Strategic Plan: 2008-2012: Synopsis*, U.S. DEP'T OF HEALTH & HUMAN SERVICES 1–3 (June 3, 2008), http://www.healthit.gov/sites/default/files/hit-strategic-plan-summary-508-2.pdf (explaining the National Coordinator's organization and its dual-purpose agenda of implementing and promoting EHR technology standards across the nation that will improve patient-focused health care, biomedical research, public health, and emergency preparedness).

[33] *See* 42 U.S.C. §§ 300jj-11(c)(3)(A)(i)–(viii) (2012) (setting forth numerous objectives that the National Coordinator is responsible for accomplishing in its efforts, such as establishing security safeguards for protecting electronic health information, making the use of health information technology more conducive to positive health outcomes, and making health information technology more user-friendly).

[34] *See, e.g.*, *Health IT Standards Committee: Recommendations to the National Coordinator for Health IT*, HEALTHIT.GOV, http://www.healthit.gov/facas/health-it-standards-committee/health-it-standards-committee-recommendations-national-coordinator (last updated Apr. 2, 2015) (providing the Standards Committee's propounded recommendations for health information technology standards).

[35] Specifically, 42 U.S.C. § 300jj-12(b)(2)(B) (2012) provides:

> [T]he HIT Policy Committee shall make recommendations for at least the following areas:
>
> (i) Technologies that protect the privacy of health information and promote security in a qualified electronic health record, including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns . . . and for the use and

Specifically, the HITECH Act tasks the Policy Committee with setting forth official standards as to how providers should document and exchange patients' "individually identifiable health information."[36]

As set forth in the Act, the Policy Committee, Standards Committee, and National Coordinator premise these standards and certification criteria on the objective of realizing the health care benefits associated with widespread use of EHRs.[37] The primary benefits of widespread implementation and employment of EHR technology include providing physicians with more comprehensive and accurate patient information, fostering improved coordination among different providers who treat the same patient, and promoting increased patient discretion in controlling their own records.[38] The HITECH Act's incentive payments, along with the benefits accompanying widespread implementation of EHRs,

> disclosure of limited data sets of such information. (ii) A nationwide health information technology infrastructure that allows for the electronic use and accurate exchange of health information. (iii) The utilization of a certified electronic health record for each person in the United States by 2014. (iv) Technologies that as a part of a qualified electronic health record allow for an accounting of disclosures made by a covered entity . . . for purposes of treatment, payment, and health care operations . . . . (v) The use of certified electronic health records to improve the quality of health care, such as by promoting the coordination of health care and improving continuity of health care among health care providers, by reducing medical errors, by improving population health, by reducing health disparities, by reducing chronic disease, and by advancing research and education. (vi) Technologies that allow individually identifiable health information to be rendered unusable, unreadable, or indecipherable to unauthorized individuals when such information is transmitted in the nationwide health information network or physically transported outside of the secured, physical perimeter of a health care provider, health plan, or health care clearinghouse. (vii) The use of electronic systems to ensure the comprehensive collection of patient demographic data, including, at a minimum, race, ethnicity, primary language, and gender information. (viii) Technologies that address the needs of children and other vulnerable populations.

42 U.S.C. §§ 300jj-12(b)(2)(B)(i)–(viii) (2012).

[36] *See id.* § 300jj-12(b)(2)(A) ("The . . . Policy Committee shall recommend the areas in which standards, implementation specifications, and certification criteria are needed for the electronic exchange and use of health information for purposes of adoption under section 300jj-14 of this title and shall recommend an order of priority for the development, harmonization, and recognition of such standards, specifications, and certification criteria . . . includ[ing] named standards, architectures, and software schemes for the authentication and security of individually identifiable health information and other information as needed to ensure the reproducible development of common solutions across disparate entities.").

[37] *See id.* §§ 300jj-11(c)(2)–(3) (providing the National Coordinator's duties, most of which ultimately highlight the benefits of EHRs and aim to improve health care quality and access by facilitating their widespread use); *see also id.* §§ 300jj-12(b)(2)(B)–(C) (putting forth the areas that the Policy Committee should consider in making its recommendations, all of which concern achieving the widespread benefits of EHR technology); *id.* § 300jj-13(b)(1)(A) (providing that the Standards Committee's recommendations as to standards and certification criteria shall be in harmony with those provided by the Policy Committee).

[38] *See Benefits of Electronic Health Records (EHRs)*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/benefits-electronic-health-records-ehrs (last updated Aug. 29, 2014) ("When fully functional and exchangeable, the benefits of EHRs offer far more than a paper record can.").

ultimately depend on health care providers' meaningful use of EHR technology. Beginning in 2015, Medicare-eligible professionals who do not meaningfully use EHRs will receive a one-percent Medicare payment reduction for that calendar year, which will increase by a percentage point for every subsequent year that the professional does not demonstrate meaningful use.[39]

B. *Meaningful Use Requirements*

The success of implementing a comprehensive EHR database hinges on whether participating professionals and hospitals actually use the technology. Incentive payments under the HITECH Act are only available to the providers that demonstrate meaningful use of EHRs.[40] According to Dr. David Blumenthal—who was the National Coordinator in 2010 when the Centers for Medicare and Medicaid Services first published the meaningful use requirements—the requirements serve as a call to action for health care providers insofar as they delineate how clinicians should use EHR technology's best features to their full potential.[41]

Pursuant to the HITECH Act, the Centers for Medicare and Medicaid Services have broken up the meaningful use requirements into three stages that providers must meet over the five consecutive years following the year that they begin the incentive payment program.[42] Thus, professionals and hospitals that started the incentive program in 2011 were required to meet meaningful use requirements for at least ninety days during the first year and for the entire year of 2012;[43] this period is Stage One.[44] After meeting

---

[39] *Medicare and Medicaid EHR Incentive Program Basics*, *supra* note 28.

[40] *See id.* ("To qualify for incentive payments, eligible professionals must successfully demonstrate meaningful use for each year of participation in the program.").

[41] *See* Blumenthal & Tavenner, *supra* note 15, at 503 ("Other core objectives include using several software applications that begin to realize the true potential of EHRs to improve the safety, quality, and efficiency of care. These features help clinicians to make better clinical decisions—and avoid preventable errors. To qualify for incentive payments, clinicians must start employing such clinical decision support tools. They must also start using the capability that undergirds much of the value of EHRs: using records to enter clinical orders and, in particular, medication prescriptions. Only when providers enter orders electronically can the computer help improve decisions by applying clinical logic to those choices in light of all the recorded patient data. And to begin extending the benefits of EHRs to patients themselves, the meaningful use requirements will include providing patients with electronic versions of their health information.").

[42] *See EHR Incentives & Certification: EHR Incentive Programs*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/ehr-incentive-programs (last updated Jan. 15, 2013) ("Maximum EHR incentives are $44,000 over five consecutive years."). For summaries of Stages One and Two of the meaningful use requirements, see *EHR Incentives & Certification: Meaningful Use Definition & Objectives*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives (last updated Mar. 18, 2014).

[43] *See My EHR Participation Timeline: 2011*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Participation-Timeline.html#.VOu541PF-Q4 (last visited Feb. 23, 2015) (noting that a provider who started meaningful use in 2011 would have to have demonstrated ninety days of Stage One meaningful use in 2011 to receive an incentive payment). That

the Stage One meaningful use requirements, providers that started in 2011 then have to meet a different set of Stage Two requirements beginning in 2014.[45] Finally, Stage Three of meaningful use commences in 2017 and will require these providers to meet a third set of requirements.[46] At the most basic level, Stage One focuses on generating protected health information in EHR format; Stage Two focuses on facilitating the exchange of such information; and Stage Three focuses on improving health outcomes with such information.[47]

Under each of the three stages, the meaningful use objectives are broken into two groups: core objectives and menu set objectives.[48] Stage One sets forth fifteen core objectives and ten menu set objectives for eligible professionals.[49] Eligible professionals must meet the fifteen required core objectives and at least five of the menu set objectives.[50] There are fourteen required core objectives for eligible hospitals and critical access hospitals and a list of ten menu set objectives.[51] Eligible hospitals must meet all fourteen core objectives and at least five of the ten menu set objectives.[52] In addition to the meaningful use objectives, eligible professionals and hospitals must report clinical quality measures, which are metrics that measure health outcomes, clinical processes, patient safety, efficiency of resource use, care coordination, and overall patient health.[53]

---

same provider would have to demonstrate a full year of Stage One meaningful use in 2012 to receive an incentive payment in that year. *Id.*

[44] *See, e.g.*, *Meaningful Use: What Do You Know?*, DEL. REGIONAL EXTENSION CENTER, http://www.dehitrec.org/Documents/MU-What%20Do%20You%20Know%20%2010%2027%2013.pdf (last visited Feb. 23, 2015) (noting that everyone must attest to at least two years of meaningful use in order to advance from Stage One to Stage Two); *see also Stage 2*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Stage_2.html (last updated Nov. 5, 2014, 3:00 PM) (noting that providers that started participating in 2011 must achieve meaningful use in three consecutive years before advancing to Stage Two).

[45] *Stage 2*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Stage_2.html (last updated Nov. 5, 2014, 3:00 PM).

[46] Neil Versel, *CMS Officially Pushes Meaningful Use Stage 3 to 2017, Offers Flexibility in 2014*, FORBES (Aug. 29, 2014, 5:00 PM), http://www.forbes.com/sites/neilversel/2014/08/29/cms-officially-pushes-meaningful-use-stage-3-to-2017-offers-flexibility-in-2014/.

[47] *See* Robert Tagalicod & Jacob Reider, *Progress on Adoption of Electronic Health Records*, CMS.GOV, http://www.cms.gov/eHealth/ListServ_Stage3Implementation.html (last updated Dec. 13, 2013, 12:41 PM) (stating that Stage One focuses on creation of health information, Stage Two focuses on exchanging that information, and Stage Three focuses on using that information to improve health outcomes).

[48] *See EHR Incentives & Certification: How to Attain Meaningful Use*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/how-attain-meaningful-use (last updated Jan. 15, 2013) [hereinafter *How to Attain Meaningful Use*] (listing meaningful use criteria for professionals and hospitals).

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *Clinical Quality Measures Basics*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/ClinicalQualityMeasures.html (last updated Sept. 18, 2014, 10:48 AM). For a comprehensive summary of all of the core objectives, menu set objectives, and

1. *Stage One*

The Stage One meaningful use requirements largely focus on capturing information that is relevant to improving patient care and transmitting it into a communicable electronic medium.[54] Participating health care providers must convert patient health records into electronic format for at least eighty percent of their patients to meet certain requirements.[55] Stage One's core objective requirements mandate that eligible professionals, hospitals, and critical access hospitals carry out a number of objectives, including but not limited to: implementing computerized provider order entry for patients' medications, providing patients with electronic copies of their own records, maintaining up-to-date records for the health status of patients, and achieving the capability to communicate with other providers regarding a patient's electronic records.[56] On an individual patient level, Stage One meaningful use criteria focus on incentivizing eligible providers to: (1) convert that patient's health information into a standard electronic format; (2) use the information to track the patient's clinical conditions; (3) convey the information to other providers treating the patient; (4) begin reporting clinical quality measures pertaining to that patient's treatment relative to a specific patient population; and (5) use the information to involve the patient and family members in making care decisions.[57] In essence, all of the Stage One requirements standardize health records into

---

clinical quality measures, see *Medicare & Medicaid EHR Incentive Program: Meaningful Use Stage 1 Requirements Overview*, CMS.GOV 6–18 (2010), *available at* http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/MU_Stage1_ReqOverview.pdf [hereinafter *Stage 1 Requirements Overview*].

[54] *How to Attain Meaningful Use*, *supra* note 48.

[55] For example, for the requirement mandating the provider to maintain an active medication allergy list, providers must have recorded at least one entry in electronic format indicating the patient's medication allergies for at least eighty percent of all patients seen by the professional or admitted to the hospital. *Stage 1 Requirements Overview*, *supra* note 53, at 11.

[56] Specifically, the Stage One core objective requirements require that each eligible professional: (1) implement computerized provider order entry for medication orders; (2) conduct drug-drug and drug-allergy interaction checks; (3) maintain an up-to-date problem list for current and active diagnoses; (4) generate and transmit electronic prescriptions; (5) maintain active medication lists; (6) maintain active medication allergy lists; (7) record each patient's preferred language, gender, race, ethnicity, and date of birth; (8) record and chart changes in each patient's height, weight, blood pressure, body mass index, and growth chart status; (9) record smoking status for patients who are thirteen years old or older; (10) "[i]mplement one clinical decision support rule relevant to specialty or high clinical priority along with the ability to track compliance with that rule"; (11) permit patients to view their records online, download, and transmit them within four business days of the information being available to the professional; (12) provide clinical summaries for each visit; and (13) "[p]rotect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities." *Ctrs. for Medicare & Medicaid Servs., Eligible Professional Meaningful Use Table of Contents Core and Menu Set Objectives: Stage 1 (2014 Definition)*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EP_MU_TableOfContents.pdf (last updated May 2014).

[57] Arthur E. Peabody, Jr., *Electronic Health Records: Technology Standards and Incentives for Meaningful Use*, *in* HEALTH CARE IT: THE ESSENTIAL LAWYER'S GUIDE TO HEALTH CARE INFORMATION TECHNOLOGY AND THE LAW 177, 200 (Arthur Peabody, Jr. ed., 2013).

electronic format and thereby make them more portable and accessible for numerous parties.

2. *Stage Two*

On a broader level, Stage Two meaningful use criteria focus on facilitating the exchange of patients' EHRs and increasing patient control over their records.[58] The Stage Two requirements are similar to their Stage One counterparts, but there are seventeen core objective requirements that eligible professionals must meet instead of only thirteen.[59] Further, the Stage Two requirements focus more on enhancing health information exchange, increasing requirements for e-prescribing, incorporating lab results into certified EHR technology, and establishing more patient control over their health information.[60] Some noteworthy Stage Two core objectives require eligible professionals to: (1) use secure electronic messaging with patients to communicate relevant health information to them; (2) achieve the capability to submit electronic data to immunization registries; and (3) provide patients with the ability to view, download, and transmit their health information online within four business days of the information being available to the professional.[61] The Stage Two core objective requirements for hospitals and critical access hospitals are similar to their Stage One counterparts, with the exception of several new ones that require hospitals to achieve the capability to submit electronic reportable laboratory results and electronic syndromic surveillance data to public health agencies.[62] Further, Stage Two sets forth new menu objective requirements, including one that mandates hospitals and professionals to record electronic notes in patient records.[63] This objective is particularly

---

[58] *See Step 5: Achieve Meaningful Use Stage 2*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/step-5-achieve-meaningful-use-stage-2 (last updated Apr. 21, 2014) ("The final rule for meaningful use Stage 2[] intends to increase health information exchange between providers and promote patient engagement by giving patients secure online access to their health information.").

[59] *Eligible Professional's Guide to Stage 2 of the EHR Incentive Programs*, CMS.GOV (Sept. 2013), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2_Guide_EPs_9_23_13.pdf.

[60] *Id.*

[61] *Stage 2 Eligible Professional (EP) Meaningful Use Core and Menu Measures: Table of Contents*, CMS.GOV (Oct. 2012), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/ Stage2_MeaningfulUseSpecSheet_TableContents_EPs.pdf.

[62] *Stage 2 Eligible Hospital and Critical Access Hospital (CAH) Meaningful Use Core and Menu Objectives: Table of Contents*, CTRS. FOR MEDICARE & MEDICAID SERVICES (Oct. 2012), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2_MeaningfulUseSpecSheet_TableContents_EligibleHospitals_CAHs.pdf. This is an optional menu objective for eligible professionals under Stage Two. *Stage 2 Eligible Professional (EP) Meaningful Use Core and Menu Measures*, *supra* note 61.

[63] *See Stage 2 Eligible Hospital and Critical Access Hospital (CAH) Meaningful Use Core and Menu Measures*, *supra* note 62 (giving eligible hospitals the option to fulfill a menu objective by recording electronic notes in patient records); *see also Stage 2 Eligible Professional (EP) Meaningful Use Core and Menu Measures*, *supra* note 61 (giving eligible professionals this same option).

relevant for purposes of health care fraud detection.[64]

The primary aim of Stage Two meaningful use criteria is to promote a nationwide electronic health information exchange.[65] The National Coordinator asserts that the primary benefit of creating such an exchange is that it homogenizes the media through which health information is transferred between providers and patients.[66] Thus, the Stage-Two meaningful use requirements premise the concept of a health information exchange upon the electronic standardization of information, which presumably enhances a provider's ability to coordinate treatment. Further, EHR technology facilitates the exchange of protected health information in several ways, including directed exchange,[67] query-based exchange,[68] and consumer-mediated exchange.[69] Theoretically, the various types of information exchange systems available under the EHR incentive program should enable a wider array of health care providers to use EHRs meaningfully and to better coordinate treatment.[70] On the other hand, this wide array of information-exchange media increases the difficulty of determining who is accessing patients' medical records and for what reasons.

3. *Stage Three*

At the time of this Note's publication, the federal government has not yet officially published the Stage Three requirements, but authorities have expressed a preliminary intent to focus the requirements on improving quality and safety to ensure better health outcomes, improve population health, provide patients with access to self-management tools, and broaden

---

[64] This is true because of some of the functional characteristics of electronic documentation methods, such as copy-paste functions. *See* Jayne O'Donnell, *Feds Push Electronic Records that Make Fraud Easier*, USA TODAY (July 6, 2014, 10:13 PM), http://www.usatoday.com/story/news/nation/2014/07/06/electronic-health-records-medicare-healthcare-fraud-funding/12157645/ (noting how recording patient records in electronic format can facilitate fraudulent documentation through the use of data cloning). I discuss some functional capabilities of EHRs that may facilitate fraud later in this Note. *See infra* Part III.C.

[65] *See* Peabody, Jr., *supra* note 57, at 200 (outlining the basic goals of the meaningful use criteria).

[66] *See Health Information Exchange (HIE): What Is HIE?*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/health-information-exchange/what-hie (last updated May 12, 2014) ("Many benefits exist with information exchange regardless of the means of [sic] which is it transferred. However, the value of electronically exchanging information is the standardization of data. Once standardized, the data transferred can seamlessly integrate into the recipients' . . . (EHR), further improving patient care.").

[67] Directed exchange is defined as the "ability to send and receive secure information electronically between care providers to support coordinated care." *Id.*

[68] Query-based exchange is defined as the "ability for providers to find and/or request information on a patient from other providers, often used for unplanned care." *Id.*

[69] Consumer-mediated exchange is defined as the "ability for patients to aggregate and control the use of their health information among providers." *Id.*

[70] *Id.*

access to a more patient-centered health information exchange.[71] The Policy Committee's Meaningful Use Work Group met in July 2012 to make initial policy recommendations for Stage Three.[72] One of the group's members, Charlene Underwood, Director of Government and Industry Affairs at Siemens Medical, emphasized the need for the Stage Three requirements to bring about a "more patient-centric solution."[73] Some notable Stage Three goals that the group contemplated include: (1) improving the tracking of individual care goals, (2) improving documentation of all persons involved in treating the patient, and (3) improving patient input in care decisions.[74]

The Centers for Medicare and Medicaid Services originally slated Stage Three to commence in 2016 but the Centers revised the timeline in December of 2013.[75] Under this new timeline, Stage Two will extend through 2016 and Stage Three will begin in 2017 for those providers who have met the Stage Two requirements for at least two years.[76] A notice of proposed rulemaking for Stage Three was to be released in the fall of 2014,[77] but the Centers for Medicare and Medicaid Services ultimately delayed and submitted a public notice of the proposed rule to the Executive Office of Management and Budget in January of 2015.[78]

---

[71] *See Draft Recommendations Meaningful Use Stage 3*, MEANINGFUL USE WORK GRP., HEALTHIT.GOV 3–6, 19, 23, 58, 60, *available at* http://www.healthit.gov/FACAS/sites/faca/files/muwg_stage3_draft_rec_07_aug_13_.v3.pdf (last visited Apr. 11, 2015) (providing various recommendations as to how to improve patient outcomes and population health using the robust health information database that should be established from completing Stages One and Two).

[72] David Raths, *MU Work Group to Make Initial Stage 3 Recommendations in August*, HEALTHCARE INFORMATICS (July 5, 2012), http://www.healthcare-informatics.com/article/mu-work-group-make-initial-stage-3-recommendations-august?WA.

[73] *Id.*

[74] *Id.*; *see* Peabody, Jr., *supra* note 57, at 200 (stating that some Stage Three goals include "[d]ecision support for national high-priority conditions[,] . . . [a]ccess to comprehensive patient data through patient-centered HIE [health information exchange, and] [i]mproving population health").

[75] Jon Mertz, *CMS Proposes New Timeline or Meaningful Use Stage 2 and Stage 3*, HL7 STANDARDS (Dec. 6, 2013), http://www.hl7standards.com/blog/2013/12/06/cms-proposes-new-timeline-for-meaningful-use-stage-2-and-stage-3/.

[76] *See* Press Release, Ctrs. for Medicare & Medicaid Servs., New CMS Rule Allows Flexibility in Certified EHR Technology for 2014 (Aug. 29, 2014), *available at* http://www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2014-Press-releases-items/2014-08-29.html ("The rule also finalizes the extension of Stage 2 through 2016 for certain providers and announces the Stage 3 timeline, which will begin in 2017 for providers who first became meaningful EHR users in 2011 or 2012.").

[77] Tagalicod & Reider, *supra* note 47; *see CMS Issues Final Rule to Extend Meaningful Use Requirements*, IHEALTHBEAT (Sept. 2, 2014), http://www.ihealthbeat.org/articles/2014/9/2/cms-releases-final-rule-to-extend-meaningful-use-requirements (discussing the potential impact of the proposed Stage Three rule on use requirements for health-care providers).

[78] Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 3, 80 Fed. Reg. 16732 (proposed Mar. 30, 2015) (to be codified at 42 C.F.R. pt. 495); Philip Peisch, *CMS Submits Proposed Rule on Stage 3 Meaningful Use to OMB*, NAT'L L. REV. (Jan. 13, 2015), http://www.natlawreview.com/article/cms-submits-proposed-rule-stage-3-meaningful-use-to-omb.

C. *Meaningful Use Enforcement*

Beginning in 2015, eligible professionals who do not meet meaningful use requirements will receive reduced Medicare physician fee schedule payments.[79] This Medicare payment reduction will begin at one percent in 2015, and it will increase to two percent in 2016 and three percent in 2017 if the professional continues not to achieve meaningful use of EHRs.[80] The payment reduction can reach up to a maximum of five percent for a Medicare-eligible professional who does not demonstrate meaningful use after 2015.[81] The Centers for Medicare and Medicaid Services will also begin penalizing eligible hospitals in 2015 if they do not demonstrate meaningful use of EHRs by reducing their Medicare payment rate as applied in their Inpatient Prospective Payment System.[82] Eligible professionals and hospitals must report their usage of EHRs annually according to the aforementioned meaningful use objectives and clinical quality measures in an electronic attestation module.[83] The Centers for Medicare and Medicaid Services determine whether the eligible professional or hospital meets the meaningful use requirements based upon their annual attestations.[84] If the Centers for Medicare and Medicaid Services suspect that a provider is making fraudulent attestations, they may subject them to an audit.[85]

Based upon the incentive payment schedule and the increasingly harsh penalties for non-compliance, the EHR Incentive Program is designed to make meaningful use of EHRs by all U.S. health care providers a reality. While the HITECH Act's meaningful use requirements are not strict insofar as they do not lead to criminal liability for noncompliance, in

---

[79] Faccenda & Parkin, *supra* note 16, at 15.

[80] *See* Peabody, Jr., *supra* note 57, at 217 (describing penalties that follow from not achieving meaningful use).

[81] *Medicare and Medicaid EHR Incentive Program Basics*, *supra* note 28.

[82] Peabody, Jr., *supra* note 57, at 217; *see* CTRS. FOR MEDICARE & MEDICAID SERVS., DEP'T HEALTH & HUMAN SERVS., ACUTE CARE HOSPITAL INPATIENT PROSPECTIVE PAYMENT SYSTEM: PAYMENT SYSTEM FACT SHEET SERIES, 3 (2013), *available at* http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/AcutePaymtSysfctsht.pdf (explaining how the IPPS payment rate for eligible hospitals is determined through a standardized formula accounting for various factors such as market conditions, costs associated with treating a beneficiary for clinical conditions, and number of readmissions).

[83] For an explanation of meaningful use attestation and an example of the attestation module format for eligible professionals, see CTRS. FOR MEDICARE & MEDICAID SERVICES, DEP'T HEALTH & HUMAN SERVS., ATTESTATION USER GUIDE FOR ELIGIBLE PROFESSIONALS: MEDICARE ELECTRONIC HEALTH RECORD (EHR) INCENTIVE PROGRAM 4, 17–29 (2014), *available at* http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/EP_Attestation_User_Guide.pdf.

[84] *See Meaningful Use Attestation*, PRACTICE FUSION, http://www.practicefusion.com/meaningful-use-attestation/ (last visited Mar. 8, 2015) (noting that eligible providers must attest to the Centers for Medicare and Medicaid Services for purposes of meeting meaningful use requirements).

[85] *Registration & Attestation*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/RegistrationandAttestation.html (last updated Dec. 29, 2014, 2:48 PM).

theory, the Act's incentive scheme enforces compliance for the large majority of health care providers who receive reimbursement payments under Medicare and Medicaid. The widespread use of EHRs is a fundamental goal underlying the HITECH Act's incentive scheme. In this vein, it is important to note that the widespread usage of EHRs changes the landscape of issues relating to data security and health care fraud.

D. *The HITECH Act's Modifications to HIPAA and Security of Protected Health Information*

The HITECH Act not only set forth an EHR incentive program, but it also implemented several changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which is the primary federal legislation that regulates the exchange of protected health information.[86] Prior to the American Recovery and Reinvestment Act's passage, if a covered entity[87] under HIPAA contracted with a business associate[88] to

---

[86] *See Summary of the HIPAA Privacy Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/ (last visited Mar. 8, 2015) (stating that the HIPAA Privacy Rule, for the first time, sets forth national standards for the use and disclosure of protected health information).

[87] Covered entities include health plans, health care clearinghouses, and "[a] health care provider who transmits any health information in electronic form in connection with a transaction covered by [Subchapter C: Administrative Data Standards and Related Requirements]." 45 C.F.R. § 160.102 (2013).

[88] Business associates include entities such as third party administrators that assist in claims processing, attorneys who counsel health care providers, consultants, medical transcriptionists, and health care clearinghouses that translate nonstandard health information into a standardized format. 45 C.F.R. § 160.103 (2013). This regulation further provides:

> (1) . . . [B]usiness associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement . . . in 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 for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities . . . billing, benefit management, practice management, and repricing; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. . . . (3) Business associate includes: (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity. (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate. (4) Business associate does not include: (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual. (ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance

perform services that involved the exchange of patients' health information and the business associate disclosed such information,[89] the government would not enforce HIPAA to punish such disclosure, but the covered entity would instead have to sue the business associate directly for breach of contract.[90] Pursuant to the HITECH Act, business associates—which include parties such as third party administrators for claims processing, attorneys, consultants, and accounting firms—are now subject to the same HIPAA liability as covered entities, meaning that they are subject to direct governmental enforcement if they disclose protected health information.[91] Specifically, the HITECH Act mandates that business associates comply with the HIPAA Security Rule by maintaining confidentiality of all protected health information that they create or handle, protecting against unauthorized access of such information, training their employees,[92] and implementing security measures for protecting such health information.[93]

The HITECH Act also subjects business associates to the HIPAA

> issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met. (iii) A government agency, with respect to determining for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law. (iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Id.

[89] "*Disclosure* means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." *Id.*

[90] Deven McGraw, *Summary of Health Privacy Provisions in the 2009 Economic Stimulus Legislation*, CENTER FOR DEMOCRACY & TECH. 2 (Apr. 29, 2009), https://www.cdt.org/files/pdfs/20090324_ARRAPrivacy.pdf.

[91] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5577 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164) ("[T]his final rule . . . adopts the NPRM proposal to add the term 'business associate' to . . . [several] provisions of the Enforcement Rule. . . . This is done to implement sections 13401 and 13404 of the Act, which impose direct civil money penalty liability on business associates for their violations of certain provisions of the HIPAA Rules.").

[92] *See* 45 C.F.R. §§ 164.306(a)(1)–(4) (2013) ("Covered entities *and business associates* must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (4) Ensure compliance with this subpart by its workforce." (emphasis added) (demonstrating the rules for covered entities)).

[93] *See id.* §§ 164.308(a)–(b) (setting forth the security specifications that business associates must implement in order to comply with HIPAA Security Rule).

Privacy Rule,[94] which protects patients' "individually identifiable health information"[95] from being disclosed or used for purposes other than those delineated by the Rule itself or without the patient's written consent.[96] There are two primary situations in which covered entities are required to disclose protected health information: (1) when the individual patient or a personal representative requests disclosure; or (2) when the Department of Health and Human Services is investigating compliance.[97] The Privacy Rule also permits disclosure and use of protected health information without the patient's consent in certain situations such as if such actions are required for treatment or public health research.[98] Similar to the Security Rule, the pre-HITECH Act Privacy Rule did not govern business associates insofar as they were only required to meet the disclosure provisions set forth in their contracts with covered entities.[99] The HITECH Act modified the Privacy Rule by giving it some teeth: business associates now must comply with the Privacy Rule requirements in the same manner as the covered entities with which they contract.[100] This is a crucial legal development in health information security, because business associates of covered entities might not be so adept at managing electronic health information, yet they are now similarly liable for any misuse or disclosure of protected health information.[101] Further, the Privacy Rule now requires

---

[94] *Health Information Privacy: The Privacy Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (last visited Feb. 23, 2015).

[95] 45 C.F.R. § 160.103 (2013). This regulation further provides:

> *Individually identifiable health information* is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Id. This information is used synonymously with protected health information throughout HIPAA. *Id.*

[96] *See OCR Privacy Brief: Summary of the HIPAA Privacy Rule*, HHS.GOV 4 (May 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf [hereinafter *Summary of the HIPAA Privacy Rule*] (discussing the basic principle for uses and disclosures of protected health information for purposes of the Privacy Rule).

[97] *See id.* (discussing the required disclosures of protected health information under the Privacy Rule).

[98] *Id.* at 4–5.

[99] *See* McGraw, *supra* note 90, at 2 (discussing the American Recovery and Reinvestment Act's modifications to the applicability of HIPAA to business associates of covered entities).

[100] "The additional requirements of this subchapter that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity." 42 U.S.C. § 17934(a) (2012).

[101] *See* Leon Rodriguez, *Enforcing HIPAA in the Age of Electronic Health Records: The View of the Office of Civil Rights from Its Director*, *in* HEALTH CARE IT: THE ESSENTIAL LAWYER'S GUIDE TO HEALTH CARE INFORMATION TECHNOLOGY AND THE LAW 301, 303 (Arthur Peabody, Jr. ed., 2013) ("HITECH's extension of liability to business associates improves our compliance efforts by holding

that covered entities and business associates only disclose or use the minimum amount of information necessary to achieve the purpose for which it is being used.[102] This requirement might prove to yield more HIPAA violations because business associates may not be as capable as covered entities in determining what amount of protected health information constitutes the minimum necessary to achieve a health care purpose. In addition to subjecting more parties to HIPAA liability, the HITECH Act increases requirements for instances where protected health information is breached.

1. *The Data Breach Notification Law*

Along with modifying the HIPAA Privacy and Security Rules with respect to business associates, the HITECH Act implements new requirements for breaches of secure protected health information. The HITECH Act establishes a new data breach notification requirement (data breach rule) for covered entities and business associates.[103] If there is a breach of protected health information, the data breach rule mandates that the concerned covered entities and business associates must notify the Department of Health and Human Services and the individuals whose health information was breached.[104] A breach occurs when there is an "unauthorized acquisition, access, use or disclosure of protected health information,"[105] but there are also some exceptions to the notification requirement.[106] Essentially, if the protected health information does not leave the business relationship between business associates and covered entities or if the information is encrypted, then the data breach rule does not apply.[107] The data breach rule also requires EHR software vendors to notify individual owners of protected health information and the Federal Trade Commission if the vendors discover that protected health

business associates accountable in the same manner as covered entities. Given that many of the most serious breaches occur at the business associate level, this change will greatly improve the privacy and security of health information.").

[102] 45 C.F.R. § 164.502(b) (2013); *see Summary of the HIPAA Privacy Rule*, *supra* note 96, at 10 ("A central aspect of the Privacy Rule is the principle of 'minimum necessary' use and disclosure.").

[103] 42 U.S.C. § 17932 (2012).

[104] *Id.* §§ 17932(a)–(b).

[105] McGraw, *supra* note 90, at 3.

[106] *See id.* (noting that the breach notification requirement does not apply in situations where the unauthorized person receiving protected health information could not have reasonably been expected to retain it; where the breach is unintentional within the scope of a professional relationship, and the information stays within the relationship; and where the breach is caused inadvertently by a workforce member under the authority of the covered entity or business associate, and the information does not leave the facility responsible for retaining it); *see also Breach Notification for Unsecured Protected Health Information*, CENTER FOR PRAC. IMPROVEMENT & INNOVATION (Nov. 2009), http://www.americanehr.com/Libraries/documents/hipaa_breach-notification.sflb.ashx (noting that breach notification requirement does not apply in certain situations).

[107] *Breach Notification for Unsecured Protected Health Information*, *supra* note 106.

information in their software format has been breached.[108] Covered entities that experience a breach affecting more than five hundred residents of a U.S. state or jurisdiction are required to notify popular media outlets in such jurisdiction, as well as all affected individuals.[109] Covered entities that experience such a breach must also notify the Department of Health and Human Services immediately,[110] which then must publish information regarding this breach on its website and report it to Congress.[111] In explaining its mission, the Office for Civil Rights at the Department of Health and Human Services (Health Office for Civil Rights)[112] extolled the virtues of the data breach rule by noting that it helps government authorities in systematically identifying common security vulnerabilities associated with protected health information.[113] A covered entity's or business associate's failure to notify the appropriate parties of a data breach results in a HIPAA violation, which subjects the entity to a fine that accounts for the nature and magnitude of the breach.[114] These notification requirements do not preempt state data breach requirements unless they are contrary to them, meaning that providers might have to meet additional notification requirements, depending upon their jurisdiction.[115]

---

[108] 42 U.S.C. §§ 17937(a)(1)–(2) (2012). Once the EHR software vendor has notified the Federal Trade Commission, the Commission must then notify the Department of Health and Human Services of the breach. *Id.* § 17937(d). If these notification requirements are not met, such failure will be prosecuted as "an unfair and deceptive act or practice in violation of a regulation under section [18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B))] regarding unfair or deceptive acts or practices." *Id.* § 17937(e).

[109] *Id.* § 17932(e)(2); *Health Information Privacy: Breach Notification Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotification rule/ (last visited Feb. 24, 2015).

[110] McGraw, *supra* note 90, at 4.

[111] *Id.*

[112] The Office of Civil Rights is a division of the Department of Health and Human Services that is responsible for enforcing laws related to civil rights in the context of health care and health information privacy. *Office for Civil Rights: OCR's Mission and Vision*, HHS.GOV, http://www.hhs.gov/ocr/office/about/mission-vision.html#mission (last visited Jan. 29, 2015).

[113] *See* Rodriguez, *supra* note 101, at 302–03 ("We now have a record of the breach notifications that we have received. These notifications have offered both OCR and covered entities vital insights into the root causes of security vulnerabilities affecting health records. While some breach reports have led to enforcement actions, we have utilized breach reports mainly to ensure that the reporting entities take corrective action and to deepen our understanding of the operational issues surrounding HIPAA compliance.").

[114] *See* 42 U.S.C. § 17939(a)(2) (2012) ("Any violation by a covered entity under thus [sic] subchapter is subject to enforcement and penalties under section 1176 and 1177 of the Social Security Act.").

[115] McGraw, *supra* note 90, at 4.

2. *Strengthened Security Enforcement*

Another way in which the HITECH Act encourages increased security of protected health information is by strengthening the penalties for security and privacy violations.[116] The Act established a tiered system of monetary penalties for providers that commit HIPAA violations.[117] At the lowest tier, a provider who does not know but should have known by "exercising reasonable diligence" that they violated a privacy or security provision is fined $100 for each violation.[118] At the highest tier, a provider who committed a HIPAA violation due to "willful neglect" and did not take action to correct it can be subjected to a $50,000 fine for each violation.[119] The HITECH Act also requires the Department of Health and Human Services to conduct periodic audits of covered entities and business associates to make sure that they comply with HIPAA requirements.[120] These audits may also lead to enforcement actions, which theoretically should bolster health information security through deterrence.[121] The Health Office for Civil Rights has already begun to conduct audits of covered entities to make sure that they have adequate procedures in place for handling health information breaches.[122]

The HITECH Act's Omnibus Final Rule[123] went into effect on March 26, 2013 and it grants the Health Office for Civil Rights authority to investigate protected health information breaches.[124] In addition to setting forth the data breach rule and the tiered monetary penalties discussed *supra*, the Omnibus Final Rule also requires covered entities and business

---

[116] Sarah E. Swank, *Enforcement Under HIPAA and HITECH: Why You Need to Worry* Again *About HIPAA*, *in* HEALTH CARE IT: THE ESSENTIAL LAWYER'S GUIDE TO HEALTH CARE INFORMATION TECHNOLOGY AND THE LAW 287, 288 (Arthur Peabody, Jr. ed., 2013).

[117] *Id.* at 288–89.

[118] 42 U.S.C. § 1320d-5(a) (2012); Swank, *supra* note 116, at 289 tbl.17.1.

[119] 42 U.S.C. § 1320d-5(a); Swank, *supra* note 116, at 289 tbl.17.1.

[120] 42 U.S.C. § 17940 (2012).

[121] The former director of the Health Office for Civil Rights, Leon Rodriguez, opined that "the use of our audit capability gives us insights into issues that we cannot readily see in our complaint-driven investigations but that often are the issues that pose the greatest threat to health information security." Rodriguez, *supra* note 101, at 303.

[122] *See, e.g.*, *Health Information Privacy: HIPAA Privacy, Security, and Breach Notification Audit Program*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa /enforcement/audit/index.html (last visited Jan. 16, 2015) (noting that in 2011, the Health Office for Civil Rights evaluated and assisted over a hundred covered entities regarding policies for notifying consumers and the government in the event of health information breaches); *see also* Swank, *supra* note 116, at 290 (describing the Health Office for Civil Rights' pilot audit program and noting that "[f]or all entities, Security Rule compliance problems posed greater difficulties than Privacy Rule compliance problems").

[123] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

[124] *See* Swank, *supra* note 116, at 292 (explaining the complaint process for notifying the Health Office for Civil Rights of a breach and the subsequent investigation that the Office conducts in response to such complaints).

associates to engage in corrective action plans, which streamline the entities' security procedures with respect to protected health information and EHRs.[125] Since the Privacy Rule's initial compliance date in April 2003, the Health Office for Civil Rights has received over 80,836 HIPAA complaints and has resolved 19,726 privacy cases as of April 2013.[126] Some of the most prevalent issues reported in the HIPAA complaints included "[i]mpermissible use and disclosures of [protected health information]," a lack of security safeguards for electronic protected health information, and excessive use of such information for unauthorized purposes.[127] Many of these complaints—which the Health Office for Civil Rights brought against a wide variety of health care providers, including large health care conglomerates,[128] private practices,[129] hospitals,[130] and government agencies[131]—developed into enforcement actions that ended in settlements.

The level of government security enforcement related to EHRs generally has increased in the wake of the Omnibus Final Rule.[132] In the pre-HITECH Act era, the Department of Health and Human Services and the Department of Justice cooperated with each other to investigate HIPAA complaints and to conduct criminal investigations.[133] The HITECH Act—through its data breach notification requirements and audit programs—has implemented government regulatory agendas from various angles to control HIPAA violations and prosecute criminals in the health care field.[134] Not only does the HITECH Act increase the enforcement power of

---

[125] *See id.* at 293 (describing the corrective action plan's purpose and goal of enticing health care entities to modify EHR policies and procedures that violate HIPAA).

[126] *Id.*

[127] *Id.*

[128] *See id.* at 294 (noting the BlueCross and Blueshield of Tennessee settlement for $1.5 million in March of 2012).

[129] *See id.* at 294–95 (noting the Phoenix Cardiac Surgery, P.C. settlement for $100,000 in April of 2012).

[130] *See id.* at 294 (noting the Hospice of North Idaho settlement for $50,000 in January of 2013).

[131] *See id.* at 295–96 (noting the Alaska Department of Health and Social Services settlement for $1.7 million in October 2009).

[132] *See* Press Release, U.S. Dep't Health & Human Servs., New Rule Protects Patient Privacy, Secures Health Information (Jan. 17, 2013), *available at* http://www.hhs.gov/news/press/2013pres/01/20130117b.html ("The final omnibus rule . . . strengthens the government's ability to enforce [HIPAA].").

[133] Swank, *supra* note 116, at 288.

[134] *See id.* ("The HITECH Act added an audit protocol that gave OCR affirmative authority to audit covered entities and business associates. In addition, the HITECH Act clarified DOJ's authority to prosecute federal criminal activity related to HIPAA, while extending enforcement authority for civil violations of HIPAA to the state attorneys general. Finally, the HITECH Act expanded those entities directly regulated under HIPAA to include business associates, who previously contractually agreed to HIPAA compliance through business associate agreements with covered entities. Enforcement of the violation of federal statutory protections by covered entities and business associates will only increase with the Omnibus Final Rule, which went into effect on March 26, 2013. All these provisions evidence an intent to protect PHI and the privacy of individuals served by health care providers across the nation.").

federal authorities, but it also grants state attorneys general the authority to enforce HIPAA regulations related to privacy and security of protected health information.[135] Further, state attorneys general have authority to enforce state laws with respect to protected health information,[136] but the Department of Justice is primarily responsible for prosecuting criminal cases related to HIPAA.[137]

The Federal Bureau of Investigation also retains authority to investigate and prosecute fraud and other criminal activities in the health care field.[138] In light of the HITECH Act's focus on promoting increased enforcement against health care fraud and HIPAA violations, the Federal Bureau of Investigation formed a partnership with the Department of Health and Human Services[139] and the Department of Justice called the HHS Health Care Fraud Prevention and Enforcement Action Team Task Force.[140] One of the first criminal convictions for a HIPAA violation after the HITECH Act occurred in April 2010, when the Federal Bureau of Investigation concluded an investigation into a former UCLA Healthcare System employee who—after being discharged—had illegally read EHRs of celebrities and high-profile patients.[141] The former employee pleaded guilty to four misdemeanor counts of violating the HIPAA Privacy Rule and was sentenced to four months in federal prison.[142] Despite the HITECH Act's enhancement of HIPAA enforcement and implementation of security measures, breaches of protected health information still occur on a wide scale throughout the United States.

---

[135] *Id.* at 296; *see* 42 U.S.C. § 1320d-5(d) (2012) ("[I]n any case in which the attorney general of a State has reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates a provision of this part, the attorney general of the State, as parens patriae, may bring a civil action on behalf of such residents of the State in a district court of the United States . . . (A) to enjoin further such violation by the defendant; or (B) to obtain damages on behalf of such residents of the State . . . ."). For a discussion of parens patriae standing in relation to other standing doctrines, see generally Kaitlin Ainsworth Caruso, *Associational Standing for Cities*, 47 CONN. L. REV. 59 (2014).

[136] *See* 42 U.S.C. § 1320d-5(d)(5) ("For purposes of bringing any civil action under paragraph (1), nothing in this section shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State."); Swank, *supra* note 116, at 296–97 (noting that the HITECH Act encourages state attorneys general to cooperate with the Health Office for Civil Rights in enforcing the security of protected health information).

[137] Swank, *supra* note 116, at 297.

[138] *See id.* at 298 (noting that the Federal Bureau of Investigation retains special units and field offices across the country to investigate crime and fraud in the health care industry).

[139] Specifically, the Office of the Inspector General. *Id.*

[140] *Id.*

[141] *Id.* at 299.

[142] *Id.*

3. *Data Breaches Abound*

The HITECH Act's data breach rule fosters accountability for misuse or loss of protected health information, but it has not stopped these problems from occurring in the first place. Loss or theft of mobile electronic devices is a primary way in which data breaches occur within the ambit of the HITECH Act. Some common examples include: backup tapes, desktop or laptop computers, and computer components containing EHRs being lost by or stolen from the health care provider.[143] In September 2011, 4.6 million records were breached when backup tapes were stolen from government health care organizations.[144] In February 2011, 1.7 million records were breached when backup tapes were stolen from Jacobi Medical Center in Bronx, New York.[145] In October 2011, 1.6 million records were breached when three backup tapes went missing from Nemours, a children's health organization in Delaware.[146] In April 2012, 315,000 records were breached when ten backup tapes were stolen from Emory University Hospital in Georgia.[147] In March 2011, 300,000 records were breached when backup tapes were stolen from the Cord Blood Registry.[148]

As for desktop or laptop computers, 4.2 million records were breached in November 2011 when a desktop computer was stolen from Sutter Physicians Service and Foundation in California.[149] In September 2009, 1 million records were breached when a computer was stolen from the Oklahoma Department of Human Services.[150] In October 2009, 850,000 records were breached when a laptop was stolen from BlueCross BlueShield/Highmark.[151] In April 2011, 514,000 records were breached when a computer was stolen from the Eisenhower Medical Center in California,[152] and 133,000 records were breached when a laptop was stolen

---

[143] Two million records were breached in March 2011 when HealthNet and IBM lost server drives in California. Lucy L. Thomson, *Health Care Data Breaches and Information Security: Addressing Threats and Risks to Patient Data*, *in* HEALTH CARE IT: THE ESSENTIAL LAWYER'S GUIDE TO HEALTH CARE INFORMATION TECHNOLOGY AND THE LAW 253, 255–56 (Arthur Peabody, Jr. ed., 2013). One and a half million records were breached in November 2009 when HealthNet lost portable hard drives in Connecticut. *Id.* A million records were breached in October 2009 when hard drives went missing from BlueCross BlueShield in Tennessee. *Id.* Eight hundred thousand records were breached in March 2012 when computer devices were lost at the California Department of Child Support. *Id.* In April 2011, 93,500 records were breached when hard drives were lost at the Mid-State Medical Center in Connecticut. *Id.* Fifty thousand records were breached in March 2013 when a contractor of the North Carolina Department of Health and Human Services lost a thumb drive. *Id.*

[144] *Id.* at 256.

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id.*

from the Oklahoma Department of Health.[153] In February 2011, 84,000 records were breached when a computer was stolen from the Saint Francis Hospital in Oklahoma.[154] In November 2011, 63,000 records were breached when a laptop was stolen from the Neurological Institute of Savannah in Georgia.[155] In January 2013, 57,000 records were breached when a laptop was stolen from the Stanford University Children's Hospital in California.[156] In March 2012, 34,500 records were breached when a laptop was stolen from Howard University Hospital in Washington, D.C.[157]

These reported breaches demonstrate that the ability to store copious amounts of data electronically in one device can be a gift and a curse. An employee simply losing a thumb drive can cause tens of thousands of EHRs to end up in an identity thief's possession.[158] The data breach rule incentivizes health care providers to be wary of such possible breaches and it encourages them to adopt security measures to prevent a breach or at least soften the repercussions arising from it.

The HITECH Act's changes to HIPAA liability are meant to bolster security and privacy measures for entities managing patient EHRs, but the Act's encouragement of increased enforcement and its establishment of a larger liability net may actually muddy the waters of health care fraud. Specifically, given that business associates and covered entities must now exercise more efforts to protect and manage EHRs, providers with fraudulent intentions might be able to point the finger at other parties in order to shield themselves from their own malfeasance. When the HITECH Act's increased liability net is coupled with the EHR incentive program that encourages more information exchange and increased patient access to protected health information, fraudsters have even more parties to blame for inconsistencies in medical records. For example, if federal authorities investigate a doctor who fraudulently bills Medicare on a routine basis, the doctor might defend himself by contending that another party such as the patient, herself, or a third party billing administrator—who now all have increased access to patient EHRs in the wake of the HITECH Act—was responsible for causing a glitch in the patient's EHR record that led to the higher amount being billed. Investigators of health care fraud should be cognizant of instances like these where the HITECH Act and increased use of EHRs changes the landscape for security and fraud liability.

---

[153] *Id.*
[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] *Id.*
[158] *See id.* (discussing the effects of a March 2013 breach at the North Carolina Department of Health and Human Services).

III. ELECTRONIC HEALTH RECORDS AND THE NEW TOPOGRAPHY OF HEALTH CARE FRAUD

The HITECH Act's EHR incentive program, meaningful use requirements, and HIPAA modifications strive to achieve better quality and coordination in health care. Yet, the EHR agenda that the Act advances—as well as its subjecting more parties to liability for breaches of protected health information—will significantly alter the landscape of fraud detection. Some policymakers, prosecutors, and commentators express concern over the ways in which EHRs may assist health care providers to commit fraud because the HITECH Act does not thoroughly address this issue.[159] Although the HITECH Act strengthens law enforcement efforts with respect to medical identity theft and protection of patients' EHRs, it does not address some of the new legal problems that its desired outcomes may manifest. One such problem that will come to the forefront in the Act's wake is the increased burden on prosecutors and auditors to detect fraud in EHRs.

A. *Health Care Fraud: Civil Penalties Under the False Claims Act*

The primary legislation that punishes perpetrators of health care fraud is the False Claims Act,[160] a statute originally enacted during the Civil War-era that Congress has broadened to encompass a wide array of fraudulent activity against the federal government.[161] Section 3729 of the False Claims Act allows for treble damages and imposes a $5,000 to $10,000 fine upon any person who, *inter alia*, "knowingly presents, or

---

[159] *See, e.g.*, Mike Miliard, *Providers Respond to Holder, Sebelius on 'Troubling Indications' of EHR Fraud*, HEALTHCARE IT NEWS (Sept. 26, 2012), http://www.healthcareitnews.com/news/providers-respond-holder-sebelius-troubling-indications-ehr-fraud (noting that U.S. Attorney General Eric Holder and Health and Human Services Secretary Kathleen Sebelius warned against using EHRs for fraudulent purposes and reporting that some health care professionals expressed dissatisfaction over the lack of guidance from the Centers for Medicare and Medicaid Services concerning protection against EHR fraud); *OIG: CMS Should Improve Efforts to Detect, Prevent Fraud in EHRs*, IHEALTHBEAT (May 29, 2014), http://www.ihealthbeat.org/articles/2014/5/29/oig-cms-should-improve-efforts-to-detect-prevent-fraud-in-ehrs ("The Office of the National Coordinator for Health IT and CMS should develop a comprehensive plan to better address fraud vulnerabilities in electronic health records, according to a report released Tuesday by the HHS Office of the Inspector General . . . .").

[160] False Claims Act, Pub. L. No. 111-21, 123 Stat. 1621 (1863) (codified as amended at 31 U.S.C. §§ 3729–3733 (2012)).

[161] *See* CHARLES DOYLE, CONG. RESEARCH SERV., R40785, QUI TAM: THE FALSE CLAIMS ACT AND RELATED FEDERAL STATUTES 5–8 (Aug. 6, 2009) (discussing the origins and development of the False Claims Act as of 2009); *see also* Joan H. Krause, *"Promises to Keep": Health Care Providers and the Civil False Claims Act*, 23 CARDOZO L. REV. 1363, 1369–70 (2002) ("The FCA was enacted in 1863 in response to 'rampant fraud' perpetrated on the Union Army during the Civil War. Almost 140 years later, multiple amendments have expanded the law beyond its modest military origins to encompass virtually any individual or entity that transacts business with the federal government. The current version of the FCA prohibits a variety of fraudulent activities involving government funds." (internal citations omitted)).

causes to be presented, a false or fraudulent claim for payment or approval" or who makes a materially false statement to the government.[162] Thus, the False Claims Act can subject offenders to significant monetary penalties, especially those who are health care providers submitting thousands of claims per year to the federal government through programs like Medicare and Medicaid.[163] The False Claims Act allows for parties to bring *qui tam* actions,[164] which permit whistleblowers[165] to sue perpetrators of fraud on behalf of the government.[166] The False Claims Act's allowance

---

[162] *See* 31 U.S.C. § 3729(a)(1) (2012) ("[A]ny person who—(A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; (C) conspires to commit a violation of subparagraph (A), (B), (D), (E), (F), or (G); (D) has possession, custody, or control of property or money used, or to be used, by the Government and knowingly delivers, or causes to be delivered, less than all of that money or property; . . . or (G) knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government, is liable to the United States Government for a civil penalty of not less than $5,000 and not more than $10,000, . . . plus 3 times the amount of damages which the Government sustains because of the act of that person."); *see also id.* § 3729(b) ("For purposes of this section—(1) the terms 'knowing' and 'knowingly' —(A) mean that a person, with respect to information—(i) has actual knowledge of the information; (ii) acts in deliberate ignorance of the truth or falsity of the information; or (iii) acts in reckless disregard of the truth or falsity of the information; and (B) require no proof of specific intent to defraud; (2) the term 'claim'—(A) means any request or demand, whether under a contract or otherwise, for money or property and whether or not the United States has title to the money or property, that—(i) is presented to an officer, employee, or agent of the United States; or (ii) is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest, and if the United States Government—(I) provides or has provided any portion of the money or property requested or demanded; or (II) will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded; and (B) does not include requests or demands for money or property that the Government has paid to an individual as compensation for Federal employment or as an income subsidy with no restrictions on that individual's use of the money or property; (3) the term 'obligation' means an established duty, whether or not fixed, arising from an express or implied contractual, grantor-grantee, or licensor-licensee relationship, from a fee-based or similar relationship, from statute or regulation, or from the retention of any overpayment; and (4) the term "material" means having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property.").

[163] *See* Krause, *supra* note 161, at 1370 (describing how health care providers can be subjected to much larger fines under the False Claims Act than other typical offenders like defense contractors because of the nature of health care providers' business).

[164] *Qui tam* actions allow private citizens to bring civil actions against defendants in order to enforce a federal statute. Thus, while private citizens bring these actions, they are essentially brought on behalf of the U.S. government as well. *See* Evan Caminker, Comment, *The Constitutionality of* Qui Tam *Actions*, 99 YALE L.J. 341, 341 (1989) ("The *qui tam* action offers an unconventional means by which Congress may enlist the aid of private citizens in enforcing Federal statutory schemes. In such an action, a private person maintains a civil proceeding on behalf of both herself and the United States to recover damages and/or to enforce penalties available under a statute prohibiting specified conduct. The private plaintiff shares any monetary recovery with the United States." (internal citation omitted)).

[165] They are also referred to as "relators" under the False Claims Act. *See, e.g.*, 31 U.S.C. § 3733(a)(1) (2012) ("Any information obtained by the Attorney General or a designee of the Attorney General under this section may be shared with any qui tam relator if the Attorney General or designee determine it is necessary as part of any false claims act investigation." (footnote omitted)).

[166] *Id.* Further, "[a] person may bring a civil action for a violation of section 3729 for the person and for the United States Government. The action shall be brought in the name of the Government." *Id.* § 3730(b)(1).

for *qui tam* actions has greatly extended the government's fraud enforcement capacity, primarily because whistleblowers can receive a percentage of any monetary penalties that offenders have to pay.[167] Furthermore, Congress recently amended the False Claims Act in its 2009 Fraud Enforcement and Recovery Act.[168] One major consequence of these 2009 amendments was Congress's expansion of liability to encompass parties who failed to reimburse the government for prior overpayment. Thus, whereas the pre-2009 False Claims Act only made parties liable once they presented a claim to get payment from the government, the post-2009 False Claims Act now covers those parties who knowingly *avoid paying back* the government.[169] In this light, the government is employing new tactics to track down and punish fraudsters. Nonetheless, it needs to double its efforts, because fraud still runs rampant.

The principles of the False Claims Act—and the Act's provision of *qui tam* actions—aim to enhance government efforts in detecting and deterring health care fraud, but many of the parties who actually blow the whistle under the Act have ulterior motives.[170] While some whistleblower claims

---

[167] *See id.* §§ 3730(d)(1)–(2) ("(1) If the Government proceeds with an action brought by a person under subsection (b), such person shall, subject to the second sentence of this paragraph, receive at least 15 percent but not more than 25 percent of the proceeds of the action or settlement of the claim, depending upon the extent to which the person substantially contributed to the prosecution of the action. Where the action is one which the court finds to be based primarily on disclosures of specific information (other than information provided by the person bringing the action) relating to allegations or transactions in a criminal, civil, or administrative hearing, in a congressional, administrative, or Government Accounting Office report, hearing, audit, or investigation, or from the news media, the court may award such sums as it considers appropriate, but in no case more than 10 percent of the proceeds, taking into account the significance of the information and the role of the person bringing the action in advancing the case to litigation. Any payment to a person under the first or second sentence of this paragraph shall be made from the proceeds. Any such person shall also receive an amount for reasonable expenses which the court finds to have been necessarily incurred, plus reasonable attorneys' fees and costs. All such expenses, fees, and costs shall be awarded against the defendant. (2) If the Government does not proceed with an action under this section, the person bringing the action or settling the claim shall receive an amount which the court decides is reasonable for collecting the civil penalty and damages. The amount shall be not less than 25 percent and not more than 30 percent of the proceeds of the action or settlement and shall be paid out of such proceeds. Such person shall also receive an amount for reasonable expenses which the court finds to have been necessarily incurred, plus reasonable attorneys' fees and costs. All such expenses, fees, and costs shall be awarded against the defendant." (footnote omitted)); *see also* HOYT W. TORRAS, HEALTH CARE FRAUD AND ABUSE: A PHYSICIAN'S GUIDE TO COMPLIANCE 67 (2d ed. 2003) ("*Qui tam* plaintiffs—sometimes referred to as relators and whistle-blowers—may personally receive 10% to 30% of the total recovery plus reasonable attorney fees. The actual percentage is determined by the court, and there are certain maximums depending on whether the government participates in the case.").

[168] Pub. L. No. 111-21, 123 Stat. 1617 (2009) (codified as amended in various sections of 18 and 31 U.S.C.).

[169] *See* Daniel C. Lumm, Comment, *The 2009 "Clarifications" to the False Claims Act of 1863: The All-Purpose Antifraud Statute with the Fun* Qui Tam *Twist*, 45 WAKE FOREST L. REV. 527, 541–42 (2010) (discussing how the Fraud Enforcement and Recovery Act modified the language in 31 U.S.C. § 3729(a)(2) to reflect that it is not required that the defendant present a claim for payment from the government in order for liability to attach).

[170] *See* TORRAS, *supra* note 167, at 68 (noting that the majority of *qui tam* actions filed against defendants under the False Claims Act are brought by disgruntled employees, spouses or significant others, and competitors).

are meritorious, many of them are not the product of a plaintiff's legitimate intent to expose fraud.[171] Nevertheless, False Claims Act whistleblower actions continue to expose a substantial amount of fraudulent activity in the health care industry. Specifically, a 2013 report indicated that the Department of Justice recovered nearly $5 billion in the 2012 fiscal year and $3.8 billion in the 2013 fiscal year through False Claims Act actions, $2.6 billion of which arose from health care fraud recovery in 2013.[172] Experience and statistics show that False Claims Act *qui tam* actions enable the federal government to recover a huge amount of money that perpetrators of health care fraud unlawfully withhold from it.[173] The annual increases in funds recovered from False Claims Act actions suggest that these actions are an important mechanism for government restitution, but the increases also demonstrate that the government is still failing to deter a large number of fraud perpetrators.

In a False Claims Act whistleblower action, the government or relator carries the burden of proof and must prove all elements and damages by a preponderance of the evidence.[174] The United States or relator must prove that the government's claim for payment was made and that the claim was false or fraudulent.[175] Courts have split on what level of intent is required for proving liability in a False Claims Act action,[176] but the general

---

[171] *See id.* at 68–69 ("An obvious danger in these suits is that disgruntled employees can blow things out of proportion, fabricate activities, or notify the government of their own improper activities that occurred without the physician's knowledge. Similarly, patients might pursue a case because they do not understand a billing statement. . . . It is hoped that attorneys soliciting business will weed out the real cases from those without merit.").

[172] A. Brian Albritton, *DOJ Announces $3.8 Billion in False Claim Act Recoveries for FY 2013*, FALSE CLAIMS ACT L. BLOG (Jan. 6, 2014, 11:33 PM), http://www.falseclaimsactlawblog.com/2014/01/doj-announces-38-billion-in-false-claim.html (citing *Justice News: Justice Department Recovers $3.8 Billion from False Claims Act Cases in Fiscal Year 2013*, DEP'T. OF JUST.: OFF. OF PUB. AFFAIRS (Dec. 20, 2013), http://www.justice.gov/opa/pr/2013/December/13-civ-1352.html).

[173] *See* Mary Jane Wilmoth, *DOJ Secures Second Largest Annual Recovery from False Claims Cases in 2013*, WHISTLEBLOWERS PROTECTION BLOG (Jan. 24, 2014), http://www.whistleblowersblog.org/2014/01/articles/false-claims/doj-secures-second-largest-annual-recovery-from-false-claims-cases-in-2013/ ("Since the inclusion of the Qui Tam provision the detection and prevention of fraud has risen exponentially. In 1986, prior to the reform, the U.S. government recovered 89 million dollars from detecting and prosecuting fraud. In 2012, that number rose to 4.95 billion dollars, 68% of that money was recovered via Qui Tam actions.").

[174] 31 U.S.C. § 3731(d) (2012).

[175] 78 AM. JUR. 3D *Proof of Facts* § 4 (2004).

[176] *Compare* United States v. Triple Canopy, Inc., 775 F.3d 628, 634 (4th Cir. 2015) (positing that False Claims Act liability requires scienter, which "encompasses actual knowledge, deliberate indifference, and reckless disregard, but does not require proof of specific intent to defraud"), *with* United States *ex rel.* Schumann v. Astrazeneca Pharms. L.P., 769 F.3d 837, 840–41, 845–46 (3d Cir. 2014) (concluding that requisite intent is knowledge), *and* United States v. Bollinger Shipyards, Inc., 775 F.3d 255, 259–60 (5th Cir. 2014) ("To meet the 'requisite scienter' requirement, the United States must plead that [defendant] acted with knowledge of the falsity of the statement, which is defined, at a minimum, as acting in reckless disregard of the truth or falsity of the information.'") (quoting 31 U.S.C. § 3729(b)(1)(A)(iii) (2012)), *and* United States *ex rel.* Grenadyor v. Ukrainian Vill. Pharmacy, Inc., 772 F.3d 1102, 1105 (7th Cir. 2014) (concluding that the requisite intent is that the defendant know the claim is false), *and* United States v. Aleff, 772 F.3d 508, 511 (8th Cir. 2014) (concluding that

consensus is that the plaintiff must prove that the defendant had actual knowledge that he was presenting a claim to the government that he knew to be false.[177] The plaintiff does not have to prove that the defendant had a specific intent to defraud the government to establish liability, but it also cannot rest its proof on the proposition that a defendant should have known that the claim was fraudulent.[178] Thus, the less stringent preponderance-of-the-evidence burden for the government may alleviate the difficulty of proving a False Claims Act violation, but the knowledge element can be particularly difficult to prove. A health care provider's recording clinical notes in electronic format can aggravate this difficulty.

B. *Health Care Fraud: Criminal Penalties*

Federal health care fraud offenses can carry a maximum punishment of life imprisonment[179] and can subject offenders to significant fines as well.[180] Health care providers may be convicted for actions such as falsifying EHR clinical notes, billing for procedures not actually performed, billing more than once for the same service, and billing for a provided service that resulted in an improper kickback to a referral source.[181] Prosecutors may charge numerous statutory violations to

---

requisite intent "includes actual knowledge, deliberate ignorance, or reckless disregard"), *and* Gonzalez v. Planned Parenthood of Los Angeles, 759 F.3d 1112, 1115 (9th Cir. 2014) ("The FCA specifically takes aim at knowing falsity, not at negligent misrepresentation.").

[177] 78 AM. JUR. 3D *Proof of Facts* § 4 (2004).

[178] *Id.*

[179] 18 U.S.C. § 1347 (2012) provides, *inter alia*, that "if the [health care fraud] violation results in death, such person [offender] shall be fined under this title, or imprisoned for any term of years or for life, or both." *Id.*

[180] *See, e.g.*, *id.* ("(a) Whoever knowingly and willfully executes, or attempts to execute, a scheme or artifice—(1) to defraud any health care benefit program; or (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program, in connection with the delivery of or payment for health care benefits, items, or services, shall be fined under this title or imprisoned not more than 10 years, or both. If the violation results in serious bodily injury (as defined in section 1365 of this title), such person shall be fined under this title or imprisoned not more than 20 years, or both; and if the violation results in death, such person shall be fined under this title, or imprisoned for any term of years or for life, or both. (b) With respect to violations of this section, a person need not have actual knowledge of this section or specific intent to commit a violation of this section."); *see also id.* § 1035(a) ("Whoever, in any matter involving a health care benefit program, knowingly and willfully—(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; or (2) makes any materially false, fictitious, or fraudulent statements or representations, or makes or uses any materially false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry, in connection with the delivery of or payment for health care benefits, items, or services, shall be fined under this title or imprisoned not more than 5 years, or both.").

[181] *Compliance Policies: Federal and State False Claims Information*, U. MD. REHABILITATION & ORTHOPAEDIC INST., http://www.umrehabortho.org/compliance/fed-state_false_claim_info.htm (last visited Jan. 13, 2015); *see* REBECCA SALTIEL BUSCH, HEALTHCARE FRAUD: AUDITING AND DETECTION GUIDE 40–41 (2d ed. 2012) (listing various forms of provider-side health care fraud, including clustering, improper modifier codes, kickbacks, and patient dumping); *see generally* Susan P. Hanson & Bonnie S. Cassidy, *Fraud Control: New Tools, New Potential*, 77 J. AHIMA 24 (Mar. 2006), *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_030850.

penalize health care fraud, but HIPAA established several specific health care fraud crimes in various sections of Title 18 of the United States Code.[182] While prosecutors have discretion as to which statutory violation to charge a perpetrator of health care fraud with committing, Section 1347 of Title 18 is often broadly applicable. In order to prove a Section 1347 violation, a prosecutor must prove, *inter alia*, that the defendant "knowingly and willfully execute[d], or attempt[ed] to execute, a *scheme or artifice* . . . to defraud any health care benefit program . . . in connection with the delivery of or payment for health care benefits, items, or services."[183] The elements of proof are similar to proving a violation of the mail fraud statute,[184] but they are specific to health care services. Unlike proving a False Claims Act violation, the prosecutor must prove each element of a Section 1347 offense beyond a reasonable doubt.[185] Prior to the Patient Protection and Affordable Care Act of 2010,[186] prosecutors had to prove that the defendant had a *specific intent to defraud* to convict him

---

hcsp?dDocName=bok1_030850 (noting that some examples of health care fraud include providers making healthy patients come in for unnecessary visits, submitting claims to Medicare for services more expensive than those actually provided, submitting claims for procedures or visits that never took place, and prescribing multiple medications to patients who doctor-shop).

[182] *See* 18 U.S.C. § 669(a) (2012) ("Whoever knowingly and willfully embezzles, steals, or otherwise without authority converts to the use of any person other than the rightful owner, or intentionally misapplies any of the moneys, funds, securities, premiums, credits, property, or other assets of a health care benefit program, shall be fined . . . or imprisoned not more than 10 years, or both . . . ."); *id.* § 1035(a) (criminalizing false statements relating to health care); *id.* § 1347 (criminalizing fraud in the context of provision or payment for health care benefits); *id.* § 1518(a) ("Whoever willfully prevents, obstructs, misleads, delays or attempts to prevent, obstruct, mislead, or delay the communication of information or records relating to a violation of a Federal health care offense to a criminal investigator shall be fined . . . or imprisoned not more than 5 years, or both."); *see also* Tim Drake et al., *Health Care Fraud*, 50 AM. CRIM. L. REV. 1131, 1173 (2013) (discussing HIPAA's establishment of federal felonies and misdemeanors related to health care fraud). Section 1347 is labeled as "health care fraud," Section 669 is labeled as "theft or embezzlement in connection with health care," Section 1035 is labeled as "false statements relating to health care matters" and Section 1518 is labeled as "obstruction of criminal investigations of health care offenses . . . ." *Id.*

[183] 18 U.S.C. § 1347(a) (2012) (emphasis added); Ellen Podgor, *The Patient Protection and Affordable Care Act of 2010 Reduces the Criminal Mens Rea Requirement for Healthcare Fraud and Increases Penalties Under the Federal Sentencing Guidelines*, WHITE COLLAR CRIME PROF BLOG (Sept. 6, 2010), http://lawprofessors.typepad.com/whitecollarcrime_blog/2010/09/the-patient-protection-and-affordable-care-act-of-2010-reduces-the-criminal-mens-rea-requirement-for.html; *see* Drake et al., *supra* note 182, at 1173 (citing United States v. Hunt, 521 F.3d 636, 645 (6th Cir. 2008) (stating the elements required to prove a Section 1347 violation)).

[184] *See* 18 U.S.C. § 1341 (2012) (providing that it shall be a crime to commit mail fraud); Samuel A. Newman & Robert G. Kidwell, *Mail and Wire Fraud*, 37 AM. CRIM. L. REV. 707, 710–11 (2000) ("[T]o convict a defendant for violating § 1341, the government must prove beyond a reasonable doubt that the defendant perpetrated (1) a scheme to defraud, (2) with the intent to defraud, (3) while using the United States mails or a private interstate commercial carrier to further that scheme.").

[185] *See Model Criminal Jury Instructions: Fraud Offenses – Mail, Wire, Bank and Health Care (18 U.S.C. §§ 1341, 1343, 1344, 1347)*, U.S. COURT OF APPEALS FOR THE THIRD CIRCUIT 39 (2014), http://www.ca3.uscourts.gov/sites/ca3/files/2013%20Chap%206%20Fraud%20Offenses%20final%20revision%202%202014.pdf (providing the elements and standard of proof for proving a Section 1347 violation).

[186] Pub. L. No. 111–148, 124 Stat. 119 (2010) (codified as amended in scattered sections of 20, 21, 25, 26, 28, 29, 30, 36, and 42 U.S.C.).

under Section 1347.[187] The Affordable Care Act abrogated the specific intent requirement, but prosecutors still have to meet the difficult burden of proving that a defendant executed a "scheme or artifice to defraud."[188] Thus, a prosecutor may have less difficulty proving health care fraud insofar as she does not have to prove specific intent, but EHRs can still make a prosecutor's job difficult in proving a scheme or artifice to defraud.

C. *Electronic Disguises of Health Care Fraud*

By design, the HITECH Act's EHR incentive and meaningful use programs encourage the widespread use of EHR software among health care providers. In certain instances, these programs also expressly encourage health care providers to alter their standard practices in ways that upend traditional fraud detection. For example, the Stage Two meaningful use menu objective that requires eligible hospitals to record electronic progress notes in patient records might make detection of language suggesting a scheme to defraud more difficult.[189] Thus, when such legislative initiatives expressly encourage providers to use functional characteristics of EHR technology in ways that change the format of traditional practices, fraudsters whose practices were becoming more apparent on paper might seize the opportunity to switch to using new electronic techniques, requiring prosecutors to go back to square one. At the very least, prosecutors will have to reassess their strategies. As one former prosecutor indicated in a recent interview concerning EHRs, some

---

[187] *See* Podgor, *supra* note 183 (explaining how the Affordable Care Act loosened the proof of intent requirement for health care fraud convictions).

[188] *See* 42 U.S.C. § 1346 (2012) ("[T]he term 'scheme or artifice to defraud' includes a scheme or artifice to deprive another of the intangible right of honest services."); *see also* United States v. Colton, 231 F.3d 890, 901 (4th Cir. 2000) (discussing the essential proof of mail, bank, wire, and health care fraud cases and noting that "[w]hat is essential is proof of a 'scheme or artifice to defraud,' which can be shown by deceptive acts or contrivances intended to hide information, mislead, avoid suspicion, or avert further inquiry into a material matter"); Podgor, *supra* note 183 (noting that prosecutors still have to prove that a defendant employed a scheme or artifice to defraud in order to establish guilt).

[189] *See Stage 2 Eligible Hospital and Critical Access Hospital (CAH) Meaningful Use Core and Menu Objectives*, *supra* note 62 (requiring eligible hospitals to record electronic notes in patient records). Specifically, the Centers for Medicare and Medicaid Services require that eligible hospitals' emergency and inpatient departments record at least one electronic progress note for more than thirty percent of "unique" patients during its reporting period. *Stage 2 Eligible Hospital and Critical Access Hospital Meaningful Use Menu Set Measures Measure 2 of 6*, CMS.GOV (Oct. 2012), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/Stage2_HospitalMenu_2_ElectronicNotes.pdf. Further, the Centers for Medicare and Medicaid Services state that electronic notes are "[d]efined as electronic progress notes. CMS will rely on providers own determinations and guidelines defining when progress notes are necessary to communicate individual patient circumstances and for coordination with previous documentation of patient observations, treatments, and/or results in the [EHR]." *Id.* An example of handwritten notes that might suggest fraud occurs where a physician writes the exact same things in his clinical notes for multiple patients without any variation whatsoever. *See* Christie Moon & Christina Matsiga, *7 Red Flags for Fraud in Medical Records*, ADVANCE HEALTHCARE NETWORK (Feb. 23, 2011), http://health-information.advanceweb.com/Features/Articles/7-Red-Flags-for-Fraud-in-Medical-Records.aspx (presenting examples of fraud in medical notes).

of the automated capabilities of EHR technology, like data-cloning, can encourage fraud.[190] Although some of the functional capabilities of EHRs—such as cloning, auto-population, and cyber portability—facilitate efficient and intelligent health care, these capabilities may actually incentivize some providers to shirk documentation responsibilities. Worse yet, these capabilities may mask fraudulent practices in unprecedented ways, making it more difficult for auditors and prosecutors to weed out perpetrators of health care fraud.

1. *Copy-Paste/Cloning Functions*

Instead of having to fill out preliminary information about a particular patient for each separate visit or medical exam, the copy-paste features of EHRs allow physicians, nurses, and employees to copy information in a patient's record from a previous visit and paste it into a new record for a later visit.[191] This is merely one example of how a health care professional may utilize copy-paste features. The copy-paste function is true to form for many technological innovations: it is a bonus for improving efficiency and lowering the cost of health care, but it is also a new potential source for error and fraud.[192]

Despite its efficiency benefits, the copy-paste function of EHR technology can cause providers to commit errors in treatment, which can be significant in some cases.[193] Copying and pasting certain routine

---

[190] *See* Marianne Kolbasuk McGee, *The Role of EHRs in Healthcare Fraud: Former Prosecutor Outlines the Potential Risks*, CAREERS INFO SECURITY (Oct. 15, 2013), http://www.careersinfosecurity.com/interviews/role-ehrs-in-healthcare-fraud-i-2077 ("Under the HITECH Act's EHR incentive program, thousands of healthcare providers have been making the move to digitized record systems. Unfortunately, some of [sic] [the] automated features of EHRs can make it easier for dishonest providers to submit padded or fake claims to payers, Ruane says. 'Many healthcare record systems contain features to expedite accurate record-keeping, but those same features can be used by fraudsters to help perpetuate their fraud,' she says. For example, a healthcare provider could clone data in one patient record and add it to another record to support submitting claims to Medicare, Medicaid or private insurers for services not actually provided, says [Maureen] Ruane, who leads a new healthcare litigation, investigations and compliance practice . . . .").

[191] *See* Justin M. Weis & Paul C. Levy, *Copy, Paste, and Cloned Notes in Electronic Health Records: Prevalence, Benefits, Risks, and Best Practice Recommendations*, 145 CHEST J. 632, 633–34 (2014) (discussing the various benefits that come with the ability to copy and paste information in EHRs).

[192] *See* Erin McCann, *CMS Called out for EHR Fraud Failings*, HEALTHCARE IT NEWS (Jan. 9, 2014), http://www.healthcareitnews.com/news/cms-called-out-ehr-fraud-failings (reporting that the Office of the Inspector General highlighted copy-and-paste functionality as a common means for committing fraud in EHRs).

[193] *See, e.g.*, Jeffrey L. Masor, *Electronic Medical Records and E-Discovery: With New Technology Come New Challenges*, 5 HASTINGS SCI. & TECH. L.J. 245, 260 (2013) ("A study also identified copying and pasting as a major source of electronic medical record documentation errors. This often occurred when medical staff would copy and paste a portion of text without properly proofreading it to ensure that it was still accurate. An example includes writing that a 'patient walked for the first time' repeated for three days." (internal citations and quotation marks omitted) (citing C.R. Wier et al., *Direct Text Entry in Electronic Progress Notes*, 42 METHODS INFO. MED. 61, 63, 67 (2003)) (discussing the widespread use of copy-paste function by clinicians and provider employees in documenting medical treatment and the ensuing errors that occur)).

information in EHRs can be harmless, but in other instances, the practice can create misleading treatment records.[194] One particular study found that nine percent of the total amount of electronic medical progress notes taken for patients visiting Department of Veterans Affairs facilities were copied.[195] The same study found that of those copied notes, sixty-three percent were copied by human authors and not by a template-generated software program.[196] Thus, the widespread practice of human users copying and pasting electronic medical progress notes—as one of the Stage Two meaningful use objectives explicitly encourages[197]—might actually be a cause for concern for prosecutors in light of the likelihood that most human users of EHR technology will copy and paste information in EHR progress notes. Such copying and pasting might be completely innocent as well, but aside from fraud concerns, the practice still creates problems for health care outcomes.[198] Further, widespread copying and pasting by human health care providers can also create discovery issues in medical malpractice litigation and fraud prosecution, particularly when the identity of a transcriber is in question in a large health care facility.[199]

The copy-paste function increases the potential for error in clinical recordkeeping and creates difficulties for litigators in detecting the source of entry. In early December 2013, the Office of the Inspector General released a report that shed light on the fraud problems that copy-paste technology creates in EHR technology.[200] In the report, the Inspector

---

[194] *See* Kenric W. Hammond et al., *Are Electronic Medical Records Trustworthy? Observations on Copying, Pasting and Duplication*, 2003 AMIA ANN. SYMP. PROC. 269, 269, 272. (discussing a study of human and template-generated copying in electronic medical progress notes for patients treated in U.S. Department of Veterans Affairs health care facilities between 1993 and 2002 and finding that of the 29,386 notes from 243 cases examined, there were 2,645 copied notes (9% of total notes)).

[195] *Id.* at 272.

[196] *Id.*

[197] *See Stage 2 Eligible Hospital and Critical Access Hospital (CAH) Meaningful Use Core and Menu Objectives*, *supra* note 62 (providing that eligible hospitals are encouraged to "record electronic notes in patient records" in order to achieve Stage Two meaningful use).

[198] *See* Anne Zieger, *EMR Copy-and-Paste May Lead to Fraud, Errors*, HEALTHCARE DIVE (Dec. 10, 2013), http://www.healthcaredive.com/news/emr-copy-and-paste-may-lead-to-fraud-errors/204627/ ("While cutting and pasting data from one template or field to another is seldom an attempt to defraud anyone—it's just a workaround to save time—it's still a problem hospitals need to address systematically. Simply pushing off responsibility onto the end users doesn't address the issue adequately, though. Ultimately, if clinicians are feeling so squeezed for time that they're creating inaccuracies by cutting and pasting, maybe the EMR user interface is the problem.").

[199] *See* Masor, *supra* note 193, at 261 (citing Ralph C. Losey & Kristen A. Foltz, *Electronic Medical Records: What Are Some of the Practical Issues Lawyers Should Be Aware of During Discovery and Litigation?*, ABA HEALTH ESOURCE (June 2009), http://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/Losey.html) (pointing out the legal conundrums that copy-paste practices with EHRs create for litigators trying to identify a tortfeasor in medical malpractice cases).

[200] *See generally* OFFICE OF INSPECTOR GEN., DEP'T HEALTH HUMAN SERVS., OEI-01-11-00570, NOT ALL RECOMMENDED FRAUD SAFEGUARDS HAVE BEEN IMPLEMENTED IN HOSPITAL EHR TECHNOLOGY (Dec. 2013) [hereinafter OFFICE OF INSPECTOR GEN.] (presenting the findings of a study that involved interviewing over eight hundred hospitals that received Medicare incentive payments to

General indicated that it had contracted with RTI International,[201] a health information technology research institute, to make recommendations regarding protection of EHRs against fraud in connection with the report.[202] The Inspector General surveyed 864 hospitals and found that "only about one quarter of hospitals had policies regarding the use of the copy-paste feature in EHR technology, which, if used improperly, could pose a fraud vulnerability."[203] The report further indicated that of the hospitals that had audit log technology, only forty-four percent "recorded the method of data entry (e.g., copy-paste, direct text entry, speech recognition) when data [were] entered into the EHR."[204] Sixty-one percent of the hospitals placed the burden of ensuring accuracy of the copied and pasted information on the providers using the EHR.[205] Fifty-one percent of the hospitals also reported that they were unable to disable, restrict, or customize copy-paste functions, which several EHR vendors also confirmed in the survey.[206]

As the Inspector General's report suggests, copy-paste features place an enormous amount of confidence in the human EHR user to record accurate information. This confidence can be particularly problematic when such a user is prone to human error or intent on defrauding patients or the government. According to the Inspector General's report, the Research Triangle Institute recommended that hospitals and government investigators use audit logs to detect misuse of the copy-paste feature of EHR technology.[207] Audit log technology is one method of detecting fraud in copied and pasted EHR notes, but as the report also indicated, not all audit logs can determine the method of data entry, which is essential for determining if information was copied and pasted.[208]

From a health care fraud perspective, a prosecutor still has to prove that a defendant "*knowingly* and *willfully* executed . . . a *scheme or artifice*

---

use certified EHR technology and concluding that many hospitals had not been adequately employing anti-fraud measures such as audit logs to address fraud vulnerabilities that may be facilitated by EHR features such as copy-paste functionality).

[201] *See Health IT and Electronic Health Information Exchange*, RTI INT'L, http://www.rti.org/page.cfm/Health_Information_Technology (last visited Feb. 1, 2015) (indicating that its clients include the Centers for Medicare and Medicaid Services).

[202] OFFICE OF INSPECTOR GEN., *supra* note 200, at i.

[203] *Id.*

[204] *Id.* at 14.

[205] *Id.*

[206] *Id.*; *see* Robert Lowes, *Fraud-Wary Feds to Regulate EHR Copy-and-Paste Function*, MEDSCAPE (Dec. 10, 2013), http://www.medscape.com/viewarticle/817604 ("The OIG report suggests that many hospitals may have a hard time controlling the use of copy-and-paste. Roughly half of the hospitals surveyed said that they are unable to disable, restrict, or otherwise customize the copy-and-paste function of their EHR systems.").

[207] OFFICE OF INSPECTOR GEN., *supra* note 200, at 14.

[208] *See id.* at 9 ("[H]ospital audit logs are less likely to record the method of data entry (e.g., direct text entry, speech recognition, automated) or the original date, time, and user identification when data are copy-pasted.").

to defraud."[209] Prosecutors and federal investigators presumably had more clues to detect the requisite knowledge or scheme to defraud in handwritten medical progress notes, seeing as they could have identified a particular transcriber's handwriting or commonly used phraseology.[210] Provided that EHR technology does not identify the transcriber, copy-paste technology increasingly will deprive prosecutors of these clues in the HITECH Act era: it will allow transcribers to use another transcriber's phraseology and it will record the borrowed language in standardized handwriting. Not only will prosecutors be unable to identify a transcriber by handwriting, but they also will likely not be certain that the recorder is the actual person indicated in the EHR.[211] The aforementioned Veteran Affairs study authors noted the particular difficulty in detecting human copying edits in EHRs without the assistance of detection software.[212]

Copy-paste technology not only might create obstacles for identifying the transcriber, but it also may mislead prosecutors into proving that a provider is willfully executing a scheme to defraud when they are actually using the feature carelessly. For example, a transcriber examining a patient over a course of many years may copy and paste information from the patient's first visit into every subsequent recording in the EHR.[213] Thus, while symptoms observed on the first appointment may have been no longer present after a certain amount of visits, they still appear in the recorded notes for all of the patient's visits.[214] This phenomenon can be particularly problematic when EHR progress notes continue across

---

[209] Podgor, *supra* note 183 (emphasis added).

[210] *See generally* Moon & Matsiga, *supra* note 189 (presenting examples of fraud in medical notes).

[211] This proposition relies on the presumption that the EHR technology indicates the identity of the transcriber. Even then, a prosecutor cannot be certain that a previous user had not logged out and another person recorded the notes under their name. This is one way in which electronic progress notes might actually be counterproductive as opposed to paper notes. Of course, it may be the case that EHR technology might eventually permit clinicians to record handwritten notes in electronic format, but this does not yet seem to be a pervasive feature in EHRs.

[212] *See* Hammond et al., *supra* note 194, at 272–73 ("Unlike machine copy-artifact, human copying is hard to detect without technical aid. . . . The variety, creativity and subtlety of human copying efforts were broad. Without Copyfind-VA it would have been very difficult to distinguish valid from invalid records. With it, many innocent-appearing records raised doubts.").

[213] *See Appropriate Use of the Copy and Paste Functionality in Electronic Health Records*, AM. HEALTH INFO. MGMT. ASS'N 4 (Mar. 17, 2014), http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050621.pdf ("*However, a number of challenges and risks associated with the copy/paste function have been identified.* These include: Inaccurate or outdated information; Redundant information, which makes it difficult to identify the current information . . . ."); *see also* Robert E. Hirschtick, *Copy-and-Paste*, 295 JAMA 2335, 2335 (2006) ("Daily progress notes become progressively longer and contain senescent information. The admitting diagnostic impression, long since discarded, is dutifully noted day after day. Last month's echocardiogram report takes up permanent residence in the daily results section. Complicated patients are on 'post-op day 2' for weeks. One wonders how utilization review interprets such statements.").

[214] *See* Hirschtick, *supra* note 213 (noting how copy-paste functionality can exacerbate the accumulation of erroneous information in patient progress notes).

separate hospital admissions because it misleads other providers.[215] A different provider working off of a previous provider's inaccurate progress notes will then bill Medicare—or the patient herself—for procedures that were not medically necessary, which can be proven as fraud.[216] A prosecutor might be misled into thinking that the provider is willfully executing a scheme to defraud when, in fact, he was just basing treatment on inaccurate notes that an earlier provider recorded in an EHR. Of course, the meaningful use objective mandating that patients have more control over their own records might eliminate this problem,[217] but they are not immune from misinterpretation either. The Department of Justice and the Inspector General have already expressed a strong intent to punish fraud enabled by copy-paste technology in EHRs,[218] but its capabilities have enabled some fraudulent health care providers to circumvent the law.

2. *Auto-Population Functions*

Another functional characteristic of EHR technology that presents obstacles for fraud detection and that enables perpetrators to commit fraud is the auto-fill, or auto-population feature. Similar to the copy-paste feature in many EHR software programs, auto-population features aim to make medical documentation quicker and effortless, yet they easily propagate inaccurate and fraudulent information. Auto-population technology automatically inputs data into an EHR when a user clicks an option on a drop-down menu, checks off a box, or types a template response into a data-entry field.[219] If the user is short on time, he may simply check off one

---

[215] *See id.* ("EMR also allows the copy-and-paste function to be used across hospital admissions, so that the last note from the previous admission can be used, with additions, as the first note for a readmission. Moreover, EMR encourages everyone to copy-and-paste the notes of everyone else so that notes become the same from author to author as well as from day to day. Even consultants are assimilated into the oneness of the EMR Borg. A cardiology consultant recently copied-and-pasted the intern's note into his own, even including 'consult cardiology in AM' in his recommendations. Perhaps he meant consult a more thoughtful cardiologist.").

[216] *See* 42 U.S.C. § 1320a-7a(a)(1)(E) (2012) (providing, *inter alia*, that a provider who files reimbursement claims to the federal government for health care procedures that the provider "knows or should know are not medically necessary" is liable for civil penalties).

[217] *See* Peabody, Jr., *supra* note 57, at 200 (providing that Stage 2 requirements aim to give patients more control over their own EHRs).

[218] *See* Robert Radick, *EMRs: The New Health Care Fraud Frontier?*, FORBES (Dec. 4, 2012, 4:58 PM), http://www.forbes.com/sites/insider/2012/12/04/emrs-the-new-health-care-fraud-frontier/ ("Attorney General Holder and Secretary Sebelius bluntly warned in their letter that '[l]aw enforcement will take appropriate steps to pursue health care providers who misuse electronic health records to bill for services never provided.'") (quoting Letter from Eric H. Holder, Jr., Atty. Gen., U.S. Dep't of Just., & Kathleen Sebelius, Sec'y, U.S. Dep't of Health & Human Servs., to Richard Umbdenstock, President & CEO, Am. Hosp. Ass'n, Charles N. Kahn, III, President & CEO, Fed'n of Am. Hosps., Steve Wartman, President & CEO, Ass'n of Academic Health Ctrs., Darrell G. Kirch, President & CEO, Ass'n of Am. Med. Colls., & Bruce Siegel, President & CEO, Nat'l Ass'n of Pub. Hosps. & Health Sys. (Sept. 24, 2012) (on file with author), *available at* http://www.nytimes.com/interactive/2012/09/25/business/25medicare-doc.html).

[219] *See* Donald A. Wochna, *Electronic Medical Records: Ready or Not, Here They Come!*, OHIO STATE BAR ASS'N (Apr. 8, 2013), https://www.ohiobar.org/ForPublic/Resources/LawYouCan

box, allow data to auto-populate in other fields, and move onto another task.[220] This common practice leads to over-documentation, which "is the practice of inserting false or irrelevant documentation to create the appearance of support for billing higher level services."[221] Another instance of over-documentation might occur if there are template responses in an EHR input interface that do not entirely encapsulate a patient's condition. Instead of taking time to note all of a patient's complaints or symptoms, a careless physician or employee may simply type in a template response for one data field that auto-populates other unnecessary fields, which leads to over-billing.[222] Not only do such practices produce errors in treatment and shelter fraud, but they also damage the integrity of diagnosis techniques.[223] While these common practices may be innocuous—just like copy-paste features—they can disguise intentional fraud.

Auto-population-induced over-documentation[224] usually manifests

---

Use/Pages/Electronic-Medical-Records-Ready-or-Not-Here-They-Come.aspx (answering basic questions about EHR technology and pertinent legal issues); *see also* David B. Troxel, *Electronic Health Record Malpractice Risks*, DOCTORS CO., http://www.thedoctors.com/KnowledgeCenter/PatientSafety/articles/CON_ID_003743 (last visited Mar. 9, 2015) ("Computer-assisted documentation [for EHRs] uses point-and-click lists, drop-down menus, auto-fill, templates, and canned text to bypass natural language and produce structured progress notes.").

[220] *See generally* AHIMA, *Integrity of the Healthcare Record: Best Practices for EHR Documentation*, 84 J. AHIMA 58, 58–60 (2013), *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050286.hcsp?dDocName=bok1_050286 [hereinafter *Integrity of the Healthcare Record*] (assessing how auto-population features in EHR technology can damage the integrity of documentation).

[221] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., OEI-01-11-00571, CMS AND ITS CONTRACTORS HAVE ADOPTED FEW PROGRAM INTEGRITY PRACTICES TO ADDRESS VULNERABILITIES IN EHRS 2 (2014) [hereinafter CMS AND ITS CONTRACTORS].

[222] *See, e.g.*, Dawn Landry, *Audit Issues with Templated Documentation*, GILL COMPLIANCE SOLUTIONS BLOG (Oct. 28, 2013), http://gillcompliance.com/blog/comments/audit-issues-with-templated-documentation ("An EMR system may allow a provider to '*point and click*' through bullet points on a template unknowingly navigating to a higher level of service. For example, clicking through [sic] a template to obtain a comprehensive history and exam for an established patient who is presenting for a straightforward problem, such as an insect bite with no other complaints . . . .").

[223] *See, e.g.*, Pat Janakowski, *Electronic Medical Records: Friend or Foe?*, LABOR NOTES (July 16, 2013), http://www.labornotes.org/2013/07/electronic-medical-records-friend-or-foe (noting that nursing is "[n]ot an [e]xact [s]cience" and stating that "[w]e [nurses] didn't go into nursing in order to fill in contextual menus to comply with reimbursement requirements"); *see also* Laura Roberts, Partner, HC Healthcare Consulting, & Amy Bailey-Muckler, Dir. of Compliance at Catholic Health East, Address at the Connecticut Hospital Association's 2013 Corporate Compliance Conference: Electronic Health Records—Auditing Quality and Compliance (Apr. 2, 2013), *available at* http://www.healthlawyers.org/events/programs/materials/documents/fc12/205_muckler_roberts_slides.pdf ("The computer may become a barrier between the doctor and the patient. When the doctor fills in a computer template, it may divert attention from the patient, limit interactive conversation, and restrict creative thinking.").

[224] This phenomenon is referred to as "upcoding," which is defined as "[a] fraudulent practice in which provider services are billed for higher CPT procedure codes than were actually performed, resulting in a higher payment by Medicare or 3rd-party payors." *Medical Dictionary: Upcoding*, FREE DICTIONARY, http://medical-dictionary.thefreedictionary.com/upcoding (last visited Mar. 9, 2015). CPT codes are codes assigned to different medical procedures that can be billed to Medicare. "CPT" stands for Current Procedural Terminology. Trisha Torrey, *What Are CPT Codes?*, ABOUT.COM, http://patients.about.com/od/costsconsumerism/a/cptcodes.htm (last updated Nov. 25, 2014).

itself in the billing and insurance contexts. For example, if a patient is required to fill in a bubble sheet for a review of her systems, indicating a current level of pain on a number scale from one to ten but there is no option for "no complaints," the patient might simply not fill in any of the corresponding bubbles. [225] If that sheet also has a box for indicating that there are no complaints and the patient fails to fill it out, a hurried technician may scan the sheet into EHR format, which automatically generates corresponding entries of "negative for pain" in the pain scale, suggesting that the patient was examined.[226] Based on this information, the provider subsequently might bill Medicare for procedures that it did not actually perform. Further, this excessive information will continue in the chain of treatment, particularly in the interoperable EHR network that the HITECH Act strives to achieve.[227] Auto-population technology also permits fraud perpetrators to set an abnormally high default reimbursement rate for all visits and to rely on hurried administrative employees to downcode the level if the patient's visit requires.[228] In the busy practice of health care, it is not hard to imagine that administrative employees forget to do this, causing Medicare to be billed at an abnormally high rate. These phenomena could be pure products of carelessness. On the other hand, they present loopholes for fraudsters to exploit. Ultimately, upcoding Medicare claims constitutes fraud within the ambit of the False Claims Act,[229] and prosecutors might not be able to tell the difference between pure negligence and a scheme to defraud.

While over-documentation fraud has been easier to detect than its

---

[225] *See, e.g.*, Cheryl L. Toth, *Auto-Population Gone Wild: EMR Documentation Can Create Risky Record Keeping*, AM. ACAD. PROF. CODERS (Feb. 17, 2010), http://news.aapc.com/index.php/2010/02/auto-population-gone-wild/ (portraying a similar bubble sheet auto-fill example).

[226] *Id.*; *see Integrity of the Healthcare Record*, *supra* note 220 ("For example, the automatic generation of common negative findings within a review of systems for each body area or organ system may result in a higher level of service delivered, unless the provider documents any pertinent positive results and deletes the incorrect auto-generated entries.").

[227] *See How Does the HITECH Act Address Barriers to Information Exchange?*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/faqs/how-does-hitech-act-address-barriers-information-exchange (last updated Jan. 15, 2013) ("The HITECH Act focuses on 'interoperability,' meaning that policies, programs, and incentives must aim for EHR software and systems that can share information with other EHR software and systems."). "An interoperable EHR is one that permits the exchange of patient health information among disparate clinicians and other authorized entities in real time and under stringent security, privacy, and other protections." WILLIAM H. ROACH, JR. ET AL., MEDICAL RECORDS AND THE LAW 448 (4th ed. 2006).

[228] *See, e.g.*, Julie Malida, *Health Insurance Fraud Gets Easier; So Should Stopping It*, INS. NETWORKING NEWS, Sept.–Oct. 2011, at 33 (providing a similar example).

[229] *See* United States *ex rel.* Harris v. Bernad, 275 F. Supp. 2d 1, 3–5 (D.D.C. 2003) (denying the defendant physicians' motion to dismiss the Government's *qui tam* action alleging that they upcoded claims to Medicare in violation of the False Claims Act); *see also Preventing Fraud in Your Electronic Medical Records*, SUNERA HEALTHCARE (Jan. 2, 2014), https://healthcare.sunera.com/blog/preventing-fraud-electronic-medical-record-emr/ ("Over-documentation leads to upcoding, and submitting an upcoded claim is a fraud.").

copy-and-paste counterpart,[230] prosecutors still shoulder the same essential burden of proving an intentional and knowing "scheme or artifice to defraud" to successfully convict a perpetrator of health care fraud.[231] The auto-population feature of EHRs is also problematic for detecting fraud because not only can fraudster providers hide behind the mask of electronic documentation, but they can also cover up their tracks. Jennifer Trussell, special advisor to the Inspector General, stressed the difficulty of tracking EHR technology with auto-population features—especially without audit-trailing software—when she noted that investigators of electronic health care fraud "don't know whether the doctor checked or unchecked, whether it was the biller, the receptionist or some guy on the street."[232] If audit logs cannot detect when a perpetrator made fraudulent alterations in an EHR record, fraudsters have a green light to cover up a scheme or artifice to defraud by simply unchecking numerous boxes and saving the records in a patient's EHR.[233] In a practice using paper medical records, if suspect providers subsequently correct errors to cover up fraudulent information, they typically cross out information and make corrections.[234] In a practice using EHRs that have template and auto-population functionality, a provider with aims to defraud can make encrypted changes, which are much more complex to detect.[235]

---

[230] *See, e.g.*, Kyle Murphy, *OIG Report Shows Flaws in CMS Detection of EHR-Related Fraud*, EHR INTELLIGENCE (Jan. 9, 2014), http://ehrintelligence.com/2014/01/09/oig-report-shows-flaws-in-cms-detection-of-ehr-related-fraud/ ("On the subject of the two most common forms of EHR-related fraud, overdocumentation and copy-paste language, the CMS contractors display various degrees of competency for identifying either practice. Although overdocumentation in EHRs was more easily detected . . . copied language in these records eluded half of all the contractors surveyed.").

[231] 18 U.S.C. § 1347(a) (2012); *see* Podgor, *supra* note 183 (noting that although the Patient Protection and Affordable Care Act of 2010 relaxed the *mens rea* requirement for the federal health care fraud offense, prosecutors still must prove a scheme or artifice to defraud in order to convict a defendant).

[232] *See* Alicia Caramenico, *Healthcare Fraud Alert: 7 Trends to Watch*, FIERCEHEALTHPAYER (Nov. 20, 2013), http://www.fiercehealthpayer.com/story/healthcare-fraud-alert-7-trends-watch/2013-11-20 ("The increasing adoption of electronic health records has led healthcare into an era of 'perfectly documented fraud,' according to Trussell. Many EHR systems, for example, allow autopopulation to automatically check what the clinician did to make the diagnosis and uncheck what he or she didn't do." (quoting Jennifer Trussell)).

[233] *Id.*

[234] *See* Losey & Foltz, *supra* note 199 (discussing EHR error correction implications for discovery purposes).

[235] *See Oracle White Paper: HITECH's Challenge to the Health Care Industry*, ORACLE 7–9, 14–15 (Oct. 2011), http://www.oracle.com/technetwork/database/security/owp-security-hipaa-hitech-522515.pdf (discussing the specialized area of data encryption in EHRs and noting that even though encryption is essential for protecting the security of protected health information, it can also contribute to the complexities involved in maintaining the integrity of EHRs).

3. *Cyber Portability*

One common characteristic of EHRs that raises fraud concerns is their portability across cyber media, particularly in nationwide information networks.[236] The HITECH Act guards against some of these fraud concerns with components such as the data breach rule and protected health information security regulations. However, prosecutors should be wary of the fraud implications that the proliferation of EHRs in a nationwide network have, particularly with respect to medical identity theft. While medical identity theft may not be unique to EHRs, the proliferation of EHRs certainly may change its habitat.

The Health Care Fraud Prevention and Enforcement Action Team provides recommendations on how to spot health care fraud and devotes significant attention to medical identity theft.[237] The increased nationwide use of EHRs propelled protected health information security concerns to the forefront of policy debate. Medical identity theft is a key element driving these concerns.[238] The Attorney General of California, Kamala D. Harris, defines medical identity theft as "the fraudulent use of an individual's identifying information in a health care setting to obtain medical services or goods, or for financial gain."[239] Attorney General Harris also notes that medical identity theft occurs in numerous ways, but one common way is insider abuse of access to patient EHRs.[240] This occurs when employees, nurses, and physicians with unlawful motives use patients' protected health information to obtain insurance proceeds or bill for higher services.[241] The effects of this crime can be particularly devastating because they can create fictitious information that follows the actual patient and can harm them long after the theft occurs.[242]

According to a 2013 survey, the Medical Identity Fraud Alliance discovered that medical identity theft affects a large segment of the U.S.

---

[236] *See* David Schultz, *As Patients' Records Go Digital, Theft and Hacking Problems Grow*, KAISER HEALTH NEWS (June 3, 2012), http://kaiserhealthnews.org/news/electronic-health-records-theft-hacking/ (claiming that the proliferation of EHRs increases the risk of medical data breaches, which "can lead to everything from identity theft to billing fraud to blackmail").

[237] *See Common Scams and Identity Theft*, STOPMEDICAREFRAUD.GOV, http://www.stopmedicarefraud.gov/preventfraud/scams-identity-theft/index.html (last visited Feb. 11, 2015) (explaining common forms of health care fraud).

[238] *See* Kamala D. Harris, *Medical Identity Theft: Recommendations for the Age of Electronic Medical Records*, CAL. DEP'T. JUST. i (Oct. 2013) (noting that the "escalation" EHRs has made medical identity theft a crucial area of concern with respect to care quality).

[239] *Id.* at 1.

[240] *Id.*

[241] *Id.*

[242] *See Medical Identity Theft*, WORLD PRIVACY F., http://www.worldprivacyforum.org/category/med-id-theft/ (last visited Mar. 9, 2015) ("[Medical identity theft] is also the most difficult [identity theft crime] to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years.").

population.[243] The survey involved nearly eight hundred adults who self-reported that they or a family member were victims of medical identity theft.[244] Further, the survey's researchers found that while there were approximately 313,000 medical identity theft victims reported in 2012, they estimated that there were 1.84 million victims in 2013.[245] The Alliance projected out-of-pocket cost to these 1.84 million victims to be twelve billion dollars.[246] Over fifty percent of the adults surveyed indicated that they suffered financially from the theft, which came in the form of required reimbursements to providers who paid identity thieves, lapsed insurance coverage, and increased insurance premiums.[247] The survey's findings regarding some of the causes of the theft shed some light on how EHRs may increase vulnerability. The survey posited some of the following occurrences as the most likely causes of medical identity theft: a family member took the victim's personal medical credentials without consent (28%); a health care provider used the victim's ID to conduct fraudulent billing (22%); personal information was inadvertently provided to a scam e-mail or website (8%); a health care provider, insurer, or other related organization had a data breach (7%); and an employee working in the health care provider's office stole the victim's health information (5%).[248] Further, 14% of the participants reported that they did not know the cause of their breach.[249]

These results are startling in light of the massive proliferation of EHRs encouraged by the HITECH Act. One attractive feature of EHR technology is its cyber portability, its ability to be viewable at the stroke of a key or a click of the mouse.[250] A large majority of medical identity theft reported in the Medical Identity Fraud Alliance survey arose from instances where this same portability is a factor, such as instances involving a data breach, a provider that fraudulently bills, a fraudulent website or e-mail address, and an employee who steals.[251] EHRs might actually reduce a victim's vulnerability to theft in situations where family members stole medical credentials, but one of the meaningful use objectives for Stage Two is to

---

[243] *Medical ID Theft Rates, Costs Continue to Climb as Consumers Fail to Protect Their Info or to Report Crime—Report*, PHIPRIVACY.NET (Sept. 12, 2013, 7:11 AM), http://www.phiprivacy.net/medical-id-theft-rates-costs-continue-to-climb-as-consumers-fail-to-protect-their-info-or-to-report-crime-report/ [hereinafter *Medical ID Theft Rates*].

[244] *Id.*

[245] *Id.*

[246] *Id.*

[247] *Id.*

[248] *Id.*

[249] *Id.*

[250] *See* ROACH, JR. ET AL., *supra* note 227, at 446 (defining a component of an EHR system as "[i]mmediate electronic access to person- and population-level information by authorized users").

[251] *See Medical ID Theft Rates*, *supra* note 243, at fig.13 (positing the most likely causes of medical identity theft).

give patients more access to, and control over, their own records.[252] This raises the question: what is stopping family members from having access to these EHRs? Further, while employees with fraudulent aims might have been unable to steal large folders filled with patient X-rays, they might have much less difficulty stealing a thumb drive or burning protected health information onto a compact disc. Lastly, in light of some of the massive data breaches reported pursuant to the HITECH Act's data breach rule,[253] the data breach causes of medical identity theft are also troubling. Thus, the cyber portability of EHRs may expose protected health information to medical identity theft in new ways that prosecutors must recognize. The HITECH Act's data breach rule is an important tool for prosecutors to understand how data breaches occur,[254] but this only sheds light on one limb of the multi-limbed beast that is medical identity theft. Ultimately, prosecutors must be able to follow stolen protected health information to its end destination where end-users use it to perpetrate fraud.

IV. PRELIMINARY RECOMMENDATIONS

Given that the widespread use of EHRs is currently in progress, the federal government has already begun to address some of the aforementioned issues related to fraud in EHRs. Nevertheless, detecting and prosecuting fraud in the world of EHRs is still in its infancy, and a flexible yet responsive plan is necessary to rein in health care fraud in its various forms.

A. *Establish Guidelines and Promote Technology Education*

One of the main concerns raised in the Office of the Inspector General's January 2014 report was the lack of guidance that the Centers for Medicare and Medicaid Services had provided to Medicare contractors on how to implement policies for detecting fraud in EHRs.[255] As the Office of the Inspector General's report suggests, the Centers for Medicare and Medicaid Services should increase efforts in providing guidelines for detecting fraudulent information in EHRs.[256] Moreover, guidelines should

---

[252] *See* Peabody, Jr., *supra* note 57, at 200 (providing that one of the Stage Two criteria focuses on more patient-controlled data and one of the Stage Three criteria focuses on increasing patient access to self-management tools for their EHRs).

[253] *See supra* notes 143–58 and accompanying text (reporting data breaches affecting more than five hundred persons).

[254] 42 U.S.C. § 17932 (2012).

[255] *See* CMS AND ITS CONTRACTORS, *supra* note 221, at 9 (noting that the Centers for Medicare and Medicaid Services have not adequately communicated with contractors about detecting fraud in EHR-based claims).

[256] *See id.* at 8 tbl.3 (reporting that, *inter alia*, only one of the eight participating Medicare Administrative Contractors, one of four participating Recovery Audit Contractors, and none of the six

explain the variety of features that EHR software provides and how these features can help to perpetrate fraud. Attorneys, patients, health care providers, and their business associates should proactively educate themselves about EHR functional features and the ways in which such features can mask fraudulent billing or clinical practices. If patients, providers, and prosecutors become shrewder with EHR technology, they will be more adept in recognizing fraud and stopping it via *qui tam* actions, criminal prosecution, or internal audit proceedings.[257] The standardization of EHR formats will facilitate creating guidelines for fraud detection, but central authorities like the Centers for Medicare and Medicaid Services should always stay abreast of new technologies that develop in the world of health information. These central authorities should also share their knowledge with all anti-fraud entities with which they cooperate.

B. *Strengthen Coordinated Enforcement Approaches*

In addition to learning about the functional characteristics of EHRs, anti-fraud authorities should coordinate their efforts with numerous parties to enhance their fraud detection strategies. These anti-fraud authorities should also embrace the power of data-analysis technology in their detection efforts. In this vein, the federal government has already made some progress, as evidenced by the Centers for Medicare and Medicaid Services' Fraud Prevention System[258] and the Health Care Fraud Prevention and Enforcement Action Team. Investigators who seek to detect fraud should work together in these kinds of multipronged enforcement organizations because they are most effective in detecting and stopping fraud in its evolving forms.

Programs like the Fraud Prevention System that use predictive

---

participating Zone Program Integrity Contractors received guidance from the Centers for Medicare and Medicaid Services on over-documentation in EHRs).

[257] *See* Lisa A. Eramo, *Stopping Fraud: Detecting and Preventing Fraud in the e-Health Era*, 82 J. AHIMA 28, 30 (2011) (suggesting that health care providers and patients should become more educated on how to detect fraud in EHRs). In this vein, Congress has already enacted legislation that calls upon the Department of Health and Human Services to conduct a nationwide education initiative with respect to the security and privacy of protected health information, 42 U.S.C. § 17933 (2012), but this Note urges that such initiatives should also focus on EHR fraud detection and prevention.

[258] *See Fraud Prevention Toolkit: CMS Fraud Prevention Initiative*, CMS.GOV, http://www.cms.gov/Outreach-and-Education/Outreach/Partnerships/FraudPreventionToolkit.html (last updated July 29, 2013, 10:43 AM) ("CMS is also using a predictive analytic technology called the Fraud Prevention System to identify the highest risk claims for fraud, waste and abuse in real time that has stopped, prevented or identified $115 million in payments, resulting in an estimated $3 for every $1 spent in its very first year."); *see also* 42 U.S.C. § 1320a-7m(b) (2012) (requiring the HHS Secretary to use "predictive analytics technologies [that] shall—(1) capture Medicare provider and Medicare beneficiary activities . . . in order to—(A) identify and analyze Medicare provider networks, provider billing patterns, and beneficiary utilization patterns; and (B) identify and detect any such patterns and networks that represent a high risk of fraudulent activity").

analytics to uncover fraud[259] are crucial in the age of EHR technology. The government's adoption of fraud detection via informatics represents a step in the right direction because law enforcement officials will ultimately be better able to pierce the veil that EHRs create for fraud that was once blatant on paper. Law enforcement authorities should also develop, enhance, and use audit logs, which can accurately determine who accessed an EHR and when changes were made to it.[260] Furthermore, lawmakers and law enforcement authorities should incentivize EHR software vendors to implement anti-fraud technology into their products. Specifically, authorities could require vendors to make the baseline settings of their EHR software include user-identification features that require every user to enter clear identity information every time he or she accesses an EHR.[261] While such measures may require fraud investigators to become better versed in predictive health informatics—which is arguably a more cryptic means of detecting health care fraud—prosecutors and law enforcement officials eventually can learn to understand it and begin to notice trends, outliers, and red flags. It is also important to note, however, that anti-fraud authorities must be on the same page with each other, considering how complicated and interconnected the world of health information is at this point in time. Further, given that private citizens can bring *qui tam* actions against suspected perpetrators of fraud, the reliability of information provided to investigators and prosecutors should always be evaluated. This is why collaborative efforts involving multiple entities would be most useful in uncovering and punishing fraud.

On the prosecution-side of coordinated enforcement efforts, prosecutors must tailor their presentation of evidence, their experts, and their legal arguments to present a willful and knowing execution of a fraudulent scheme or artifice to defraud. Perhaps this is the greatest

---

[259] The Centers for Medicare & Medicaid Services' predictive analytics basically evaluate Medicare claims in real time and compute a risk score based upon various metrics like type of provider, type of service, identity of beneficiary, and patterns in claims. The Centers will then investigate potential fraud based upon that risk score. Linda Rosencrance, *How Predictive Analytics Help Fight Healthcare Fraud*, TIBCOSPOTFIRE (Nov. 1, 2011), http://spotfire.tibco.com/blog/?p=8738.

[260] *See* Masor, *supra* note 193, at 254 (discussing the utility of audit trails in determining EHR authenticity).

[261] *Cf.* AHIMA, *Privacy and Security Audits of Electronic Health Information*, 88 J. AHIMA 54, 54 (2014) ("In a perfect world, access controls alone would ensure the privacy and security of electronic protected health information (ePHI). However, the complexities of today's healthcare environment make it extremely challenging to limit access to the minimum information necessary that members of the workforce require in order to perform their jobs. In smaller organizations and community-based hospitals, employees may perform multiple functions, each of which requires different levels of access. Without having access to specific portions of every patient's health record, employees' effectiveness could be significantly inhibited, and patient care and safety could be compromised. Organizations must develop security audits and related policies and procedures to hold members of the workforce accountable for their actions when accessing ePHI through the electronic health record (EHR).").

challenge of all, but it might be more feasible as legal precedents emerge and as prosecutors become more adept at recognizing fraud in EHR format.[262] Prosecutors must get creative in presenting circumstantial evidence as well.[263] For example, prosecutors must be able to take a step back from the particularized data contained in EHRs and the corresponding billing documents.[264] Instead, prosecutors should present evidence concerning how a suspected fraud perpetrator's EHRs compare to those of other providers in the industry or in the same geographic area. In this light, prosecutors should be able to transcend the seemingly legitimate appearance that fraudulent records may have in electronic format.

Policymakers should also work in tandem with law enforcement officials and prosecutors and should be mindful of how legislative initiatives like the HITECH Act's EHR incentive and meaningful use programs may perpetuate fraud. In light of United States Senator Orrin Hatch's statement at the Committee on Finance's July 2013 hearing on health information technology, legislators should not be afraid to "push the pause button" on legislative initiatives incentivizing overtly beneficial technology.[265] While stopping the meaningful use program is not advisable, legislators should take Senator Hatch's sentiment to heart and look at the big picture surrounding legislative goals. In short, lawmakers

---

[262] Prosecutors should also rely more heavily on billing or treatment standards in a provider's particular health care industry to present evidence of abnormal practices suggesting a scheme to defraud. For a useful example of how a prosecutor proved a physician's scheme to defraud based upon medical necessity standards in the physician's industry, see United States v. Patel, 485 F. App'x 702 (5th Cir. 2012).

[263] *See id.* at 708 ("Intent to defraud is typically proven with circumstantial evidence and inferences." (citing United States v. Ismoila, 100 F.3d 380, 387 (5th Cir. 1996)). For an example of a prosecutor's successful presentation of circumstantial evidence to prove that a defendant knowingly participated in a scheme to defraud Medicaid, see United States v. Essien, 530 F. App'x 291, 299–300 (5th Cir. 2013).

[264] *See, e.g.*, BUSCH, *supra* note 181, at 273–74 ("An electronic interoperable healthcare market opens the doors to tremendous opportunities in the area of waste, fraud, and abuse. . . . The market does not move forward with respect to standards, for example, simple analyses of how many patients are being treated for a particular diagnosis. The universal billing form created this opportunity by forcing the market to submit the content of the bill in a consistent format among all providers. The standardization of the universal billing form along with sophisticated computer tools, has allowed for exploratory data analysis (EDA) opportunities of large volumes of data for waste, fraud, and abuse through comparative analysis from provider to provider and market to market.").

[265] *See Health Information Technology: A Building Block to Quality Health Care: Hearing Before the S. Committee on Finance*, 113th Cong. 6 (2013) (statement of Sen. Orrin G. Hatch) ("It would seem to me that we have an opportunity to push the 'pause' button and make sure that the [meaningful use] program is working before we continue down a potentially unsustainable path."); Press Release, Senate Comm. on Fin., Hatch Statement at Finance Committee Hearing Examining How Health Information Technology Can Improve Health Care Quality (July 17, 2013), *available at* http://www.finance.senate.gov/imo/media/doc/07%2017%2013%20Hatch%20Opening%20Statement%20on%20Health%20IT%20hearing.pdf (same); *see also* Dan Bowman, *Hatch Wants to Pause, Reassess Meaningful Use*, FIERCEEMR (July 18, 2013), http://www.fierceemr.com/story/hatch-wants-pause-reassess-meaningful-use/2013-07-18 (reporting Senator Hatch's comments at the Senate Finance Committee hearing,which expressed his concern as to whether the meaningful use program was actually saving the government money).

should never hesitate to view every legislative act related to EHRs as a double-edged sword: more widespread use of EHRs could create more exposure to potential medical identity theft via cyberspace; more patient access to EHRs could lessen physicians' ability to treat the patient; more automated data entry features could conceal fraud from prosecutors. Legislators should address all of these considerations with equal analytical vigor. Further, state legislators should not assume that Congress ultimately dictates policy related to EHR fraud. Instead, they should take the initiative to enact state laws to account for federal law deficiencies. For example, one section in the Code of Federal Regulations provides that federal provisions preempt contrary state provisions, *except* for state provisions that are "necessary . . . [t]o prevent fraud and abuse related to the provision of or payment for health care."[266] In essence, this statutory exception grants state legislators permission to experiment with legislation that addresses a nationwide policy concern.

Finally, patients should be privy to their health care providers' actions as they relate to their EHRs. HIPAA and the HITECH Act pave the way for more patient access to EHRs through the meaningful use program and patients should always be wary of inconsistencies or abnormalities in their EHRs. Further, they should restrict family members' and friends' access to their EHRs, subject to physician recommendations and physical conditions that require it.[267]

C. *Increase the Scope of Fraud Investigation*

The sweeping provisions of the HITECH Act and its HIPAA modifications suggest that the world of EHRs is becoming more interwoven. In this light, prosecutors, auditors, and other anti-fraud actors should adopt a wider perspective in looking at the timeline of protected health information in electronic format. These anti-fraud actors should also adopt a wider perspective in looking at the potential parties involved in fraudulent activity. Specifically, as for looking at the timeline of protected health information, anti-fraud investigators should be mindful of the spread of EHR adoption and they should consider the reality that many potential actors—both good and bad—might have access to EHRs. Therefore, fraud investigators should rely on audit technology and meticulously follow each and every transaction—from creation to destruction—involved in the long life of EHRs. As for looking at potential parties involved in fraud, since the HITECH Act increased the scope of HIPAA liability for protected health information breaches to include business associates of covered entities,

---

[266] 45 C.F.R. § 160.203(a) (2013).

[267] Such as if the patient is mentally challenged and needs family assistance in evaluating his or her protected health information.

anti-fraud authorities should track closely the actions of all of these involved parties to ensure that *both* covered entities *and* business associates are not perpetrating fraud. Anti-fraud authorities should also stay abreast of all data breach notifications, paying close attention to what happens to EHRs after they have been accessed, breached, and/or used for other transactions.

Further, given that the 2009 amendments to the False Claims Act greatly expanded the scope of liability for submitting false claims for payment from the government, anti-fraud authorities should look at the back end of health care transactions and should track suspect health care providers with increased vigor even after they have billed Medicare or Medicaid. Thus, as an example, if the Centers for Medicare and Medicaid Services determine that they have overpaid a particular health care provider, they should look closely at whether the provider is avoiding payment to the Centers when they seek reimbursement. In this manner, anti-fraud authorities can track down all of the various forms of fraud that afflict the modern U.S. health care industry.

V. CONCLUSION

Physicians and scientists have used EHRs since the 1960s,[268] and EHRs will become increasingly important in the world of health care for the near future. EHRs provide more comprehensive assessments of a patient's health, they save production-related costs, they standardize the means of communication between disparate providers, and they exponentially improve the speed at which protected health information travels.[269] However, EHRs present new exposures to fraud and data breaches. These exposures not only lead to financial losses, but they also lead to a diminished quality of care. If policymakers, prosecutors, and providers do not rein in these exposures and do not pierce EHR technology's electronic veil covering fraud, then the aims of the HITECH Act might become meaningless. One author points out the ironic outcome that EHR technology can manifest, stating that "with technology comes risk—and for the medical providers that . . . rely upon [EHRs], that risk may include increased scrutiny, investigation, and even prosecution by the very government that promoted the switch to [EHRs] in the first place."[270]

---

[268] *See* Robyn Weisman, *How EHR Came to Be (or Why Doctors Aren't Like Airline Pilots)*, STORAGECRAFT (Apr. 25, 2014), http://www.storagecraft.com/blog/ehr-came-doctors-arent-like-airline-pilots/ (explaining, for example, that Latter Day Saints Hospital in Utah began using software called Health Evaluation through Logical Programming (HELP) in 1967, which was an early form of EHR technology).

[269] *See* ROACH, JR. ET AL., note 227, at 440–41 (discussing the core functional characteristics of EHRs).

[270] Robert Radick, *EMRs: The New Health Care Fraud Frontier?*, FORBES (Dec. 4, 2012, 4:58 PM), http://www.forbes.com/sites/insider/2012/12/04/emrs-the-new-health-care-fraud-frontier/.

EHR technology aims to achieve a more coordinated and holistic approach to health care. We should espouse a holistic approach in analyzing EHR technology's effects on the law.