There is no neutral position on fraud!

Donald W Simborg

Correspondence to
Dr Donald W Simborg, 407 Old Downieville Hwy, Nevada City, CA 95959, USA;
dsimborg@sbcglobal.net

Received 22 February 2011
Accepted 22 April 2011
Published Online First
4 July 2011

ABSTRACT

In 2005, Dr David Brailer, our first National Coordinator for Health Information Technology, had a vision of widespread adoption of electronic health records connected through networks run by regional health-information organizations. An advisory panel recommended at that time that proactive fraud management functions be embedded in this emerging information infrastructure. This has not occurred. Currently, the agencies responsible for fraud need the assistance of the Office of the National Coordinator for Health Information Technology in order to most effectively manage the growing problem of fraud related to the adoption of electronic health records and health-information exchanges.

In 2005, Dr David Brailer, our first National Coordinator of the Office of the National Coordinator for Heath Information Technology (ONC), had a vision of widespread adoption of electronic health records (EHRs) connected through networks run by regional health-information organizations. He set out to build the underlying infrastructure for this emerging Nationwide Health Information Network (NHIN) by setting up the precursors to our current advisory committees on Health IT policy and standards, EHR certification organizations and IT standards selection processes. He even anticipated one of the possible unintended consequences of widespread IT adoption by convening a study group to look at the question of healthcare fraud as it may relate to the NHIN.

As the co-chair of the expert panel involved in this study, I remember vividly the question Dr Brailer put to our panel: 'Should the NHIN be neutral with regard to fraud or proactive in combating fraud?' Some might wonder why he would even ask such a question, given that no one (except fraudsters) condones fraud. However, it was and remains a legitimate question. The NHIN can be considered a utility. Building it is a large and complicated task. Dr Brailer had very limited funding at the time, and his focus clearly needed to be on creating the NHIN. The responsibility for fraud belongs primarily with the Centers for Medicare and Medicaid Services (CMS), the Office of the Inspector General (OIG) and the Department of Justice (DOJ) at the federal level, and one could legitimately argue that ONC should not dilute its focus by taking on that responsibility. In the subsequent report issued by our study group, we outlined a set of 'guiding principles' regarding the issue of fraud as it relates to the NHIN. The first principle was, 'The Nationwide Health Information Network (NHIN) policies, procedures, and standards must proactively prevent, detect, and support prosecution of healthcare fraud rather than be neutral to it.'[1] Thus, our panel of experts concluded that ONC in building the NHIN should not be neutral with respect to fraud. The overwhelming opinion at that time was that without proactive fraud management, EHRs and the NHIN would become agents of fraudsters, and fraud would increase.

It is now 6 years later. The leadership of ONC has chosen not to be proactive with regard to fraud management and has largely left this problem to the other agencies. There has been some activity relating to fraud at ONC. Dr Robert Kolodner, the second National Coordinator, convened a second study specifically related to EHRs and fraud.[2] He also commissioned a report by Booz Allen Hamilton on medical identity theft.[3] There are some fraud-related functions required by the Certification Commission for Health Information Technology, but these are limited to those which overlap with security and privacy concerns which motivated their inclusion. Virtually no follow-up has occurred to any of the fraud-specific recommendations in the fraud reports, the existing 5-year plan for Health IT developed by ONC has no mention of fraud,[4] and the overwhelming focus of ONC this past year has been in implementing the EHR adoption incentive program and 'meaningful use.' There is nothing in the meaningful use requirements that is fraud-related. As of this writing, ONC has published a draft of a new Federal Health IT Strategic Plan: 2011–2105 for public comment. Again, fraud management is not a part of the plan. Thus, ONC is indeed neutral with regard to fraud.

At the same time, Congress has increased its focus on fraud. The Health Care Fraud and Abuse Control Program, which includes the Health Care Fraud Prevention and Enforcement Action Team (HEAT), has been allocated additional funds from Congress and is aggressively pursuing Medicare and Medicaid fraud.[5] In addition, there are increased funds to combat fraud in the Patient Protection and Affordable Care Act. It should be pointed out that there is a wide spectrum of fraud, not all of which can be influenced by healthcare IT. The types of fraud, however, that involve false claims for clinical provider services are directly influenced by the documentation provided by EHRs. Increasingly, highly publicized sting operations and nationwide coordinated arrests of fraudsters are netting hundreds of millions of dollars in recoveries. These are valuable programs, and their publicity alone undoubtedly deters significant fraud. Further, the ROI for our investments in these programs ranges anywhere from 4/1 to 17/1, as reported in various Congressional testimonies[6]—impressive returns. However, on an absolute dollar basis, they are paltry compared to the probable size of the problem. Dan Levinson, the DHHS Inspector General, estimates that fraud recoveries are just the 'tip of the iceberg.'[7]

How much fraud is there? The simple answer is, 'we don't know.' The minimum experts have estimated is 3% of the total healthcare expenditure, with most experts estimating closer to 10%. On a $2.5T annual budget, that is an astounding amount of fraud. Compared to the banking industry, which knows its fraud loss almost down to the penny, the healthcare fraud transaction rate is 30 to 100 times greater!

Do EHRs and other healthcare IT lead to increased fraud compared to paper medical records? Again, we do not know the answer definitively. It has not been properly studied. Such studies are difficult to perform, and true controlled studies are impossible. In a meeting with OIG officials recently, I suggested that some preliminary clues could be obtained simply by performing 'case-controlled' studies of billings done by comparable clinical practices before and after conversion from paper to electronic documentation comparing to practices that remained on paper documentation. A positive result would not necessarily indicate that fraud is occurring, but it would point the way toward further investigation. A negative result would be somewhat reassuring. No such study has been published. We are therefore left with expert opinion and anecdotal evidence. Compliance officers are increasingly raising the red flag. EHR vendors, in an attempt to satisfy customer demand to facilitate charge capture and speed up encounters, have introduced a variety of tools which meet these legitimate demands but also are subject to fraud and abuse. Copy forward, record cloning, default notes, single-click template notes, 'make me an author,' and E&M code optimization alerts are just a few examples. The line between legitimate uses of these tools and fraud is sometimes blurred. Examination of user date/time stamps from audit files (metadata) from EHR encounter notes reveals instances where vital signs are entered the day before a patient's alleged visit. Entire templated notes are also entered prior to encounters, sometimes with no alteration on the day of the alleged visit. The 'make me an author' tool of one vendor allows a physician to substitute their signature attribution for another person who entered a note. One vendor has a tool to allow retroactive alteration of a note avoiding their 'amended note' designation. Some vendors allow the suspension of the recording of audit trails. Many vendors provide 'alerts' or 'advice' on upcoding E&M codes. In the spectrum of possible uses of these 'tools,' some are legitimate, and some clearly are not. Again, although not systematically reported in the literature, there is much anecdotal evidence that indicates that Medicare billings have increased after the introduction of EHRs.[8] Is this simply better coding or fraud, or a combination? We do not know.

What we do know is that identity theft of both provider IDs and patient IDs is occurring. We also know that the increasing availability of legitimate encounter notes in electronic format increases the probability of theft of encounter notes compared to paper records. With facilitated access to multiple provider organizations' EHR data through Health Information Exchanges (HIEs), more complete documentation on episodes of care can be stolen. This 'perfect storm' enables the fabrication of fraudulent claims, including the fabrication of entirely fictitious encounters with credible and fraud-detection-resistant documentation in much larger volumes than was possible previously.

CMS, OIG, and DOJ are very aware of these possible abuses of EHRs and HIEs. They are investing heavily in predictive modeling and other analytic tools to better detect these abuses. While this is going on, ONC is distributing billions of dollars in incentives to adopt these technologies in a neutral or near-neutral stance toward these same abuses. This makes no sense.

ONC needs to step up to the plate. There is no neutral position! Without proactive fraud management functions built in, fraud will increase in an electronic environment. Data captured in EHRs is the legal record of care that serves as the source of truth and the standards for EHRs are set by ONC. A little bit of help from ONC will do far more to reduce fraud than equivalent expenditures by CMS, OIG, and DOJ. What should ONC be doing that it currently is not?

1. There need to be clear guidelines regarding the use of the various EHR tools now available.
2. Certification requirements need to define not only what a vendor's product must do, but also what they should not be allowed to do.
3. There must be a credible threat of decertification if vendors enable illegitimate uses of these functions after certification.
4. The metadata now collected by most EHRs need to be better defined and standardized, and made available to the analytical systems being deployed to detect fraud.
5. Our methods for both provider and patient authentication at the time of an encounter need to be seriously reconsidered.
6. Support research focused on both characterizing fraud as it relates to EHRs and tools for promoting compliance.

All of these fraud-management functions can be best implemented by ONC. With the amount of funding now available to ONC—something Dr Brailer could not have even imagined—there is no excuse that funds are not available for this added focus. But neither ONC nor CMS/OIG/DOJ can do this alone. There needs to be *intense* collaboration between these agencies to best design the fraud-management tools and processes that must be embedded in HIEs and EHRs at the point of care. These agencies need to get out of their silos. ONC needs access to the expertise and data available within CMS/OIG/DOJ regarding our current fraud experience. This needs to be better quantified so that the fraud management tools can be properly designed and prioritized. On the other hand, CMS, OIG, and DOJ need the organizational capabilities under the control of ONC to implement and monitor the use of these tools in the field. The emphasis of ONC on defining and deploying Meaningful Use incentives has been important during the past 2 years given the timelines required by the HITECH legislation. That only increases the urgency to focus on fraud, which will continue to occur in the fee-for-service payment portions of Medicare and Medicaid, but will also occur regarding claims of Meaningful Use as well. With a new coordinator arriving for ONC, this would be a good time to shift from ONC's fraud neutral policy.

Competing interests None.

Provenance and peer review Not commissioned; externally peer reviewed.

REFERENCES

1. *Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities*. Prepared for the Office of the National Coordinator by Foundation of Research and Education, American Health Information Management Association, Chicago, Illinois, under contract from the Office of the National Coordinator for Health Information Technology, DHHS, 30 September 2005.
2. *Recommended Requirements for Enhancing Data Quality in Electronic Health Record Systems*. Report prepared by RTI International, Research Triangle Park, under contract from the Office of the National Coordinator for Health Information Technology, Department of Health and Human Services June 2007.
3. **Booz Allen Hamilton.** *Medical Identity Theft Environmental Scan*. Report prepared by Booz Allen Hamilton, Rockville, MD, under contract from the Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, 15 October 2008.
4. *ONC-Coordinated Federal Health IT Strategic Plan, 3 June 2008*. Office of the National Coordinator for Health Information Technology, Department of Health and Human Services.
5. *The Department of Health and Human Services and the Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2010*. Washington, DC: Department of Health and Human Services, January 2011.

6. *Statement of Lewis Morris, Chief Counsel, Office of the Inspector General, Department of Health and Human Services before the Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security*. Washington, DC: Senate Committee Prints, Government Printing Office, 22 April 2009.
7. *Testimony of Daniel R. Levinson, Inspector General, US Dept. of Health and Human Services, before the House Appropriations Subcommittee on Labor, Health and Human Services, Education and Related Agencies*. Washington, DC: Department of Health and Human Services, 4 March 2010.
8. **Grider D,** Linker R, Thurston S, *et al*. The problem with EHRs and coding. *Med Econ* 2009. http://www.modernmedicine.com/modernmedicine/Modern+Medicine+Now/The-problem-with-EHRs-and-coding/ArticleStandard/Article/detail/590411.