The National Health Care Anti-Fraud Association estimates that the annual cost of healthcare fraud is somewhere between 3% and 10% of total healthcare costs. That estimate is not only astounding because of its magnitude, but also because of its range, indicating uncertainty. The sum of $100B per year, one way or another, matters. For example, that difference would fund all of the imagined Nationwide Health Information Network (NHIN) in any of its possible forms and a whole lot more.

The Office of the National Coordinator for Health Information Technology (ONC) has completed two contracts related to healthcare fraud. The first, performed by the Foundation on Research and Education of the American Health Information Management Association, issued a report in 2005 in which an expert panel recommended a set of “Guiding Principles” for health information technology relating to healthcare fraud management. (“Fraud management” is defined as the prevention, detection and prosecution of fraud.)

The second contract, performed by RTI International, issued a report in 2007 in which a second expert panel recommended 14 requirements for electronic health records related to healthcare fraud management. I served as the co-chairman of the first expert panel and the chairman of the second expert panel. It is my experience with these two panels and the subsequent industry reaction that prompts the title of this paper.

In our kickoff meeting under the first contract, Dr. David Brailer, in giving the charge to our panel, asked us to answer the question, “Should the emerging NHIN play a role with regard to reducing healthcare fraud and, if so, what role?” The ensuing contract process involved an extensive review of the literature, on-site interviews with multiple healthcare stakeholders including providers, consumers, payers, healthcare economists, law enforcement, and technology organizations. The expert panel, which included representatives from all of these stakeholders, reviewed the results of this fact gathering process, heard presentations from various outside experts, and deliberated regarding Dr. Brailer’s question.

The result was a set of Guiding Principles, the first of which was, “The Nationwide Health Information Network (NHIN) policies, procedures, and standards must proactively prevent, detect, and reduce healthcare fraud rather than be neutral to it.” The reason for this conclusion was the universal opinion of the experts that the potential for fraud increases in an electronic environment and without proactive steps in fraud management, our enormous problem will get worse. Further, experience has shown that it is far more effective to prevent fraudulent payments than to pay and chase,” which is the predominant model in use today. Since we are still early in the use of EHRs and interoperable networks, now is the time to anticipate this problem.

Another Guiding Principle of the first report was, “EHR standards must define requirements to promote fraud management and minimize opportunities for fraud and abuse, consistent with the use of EHRs for patient care.” This was the basis for the second contract with RTI International which convened another expert panel to make recommendations for such requirements for EHRs. These recommendations were intended to specifically inform the processes of both the Health Information Technology Standards Panel (HITSP) and the Certification Commission for Health Information Technology (CCHIT). This second expert panel consisted of some of the panel members from the first contract plus additional stakeholders from the provider community with EHR and EHR vendor experience. The panel process involved the development of use cases for the commitment of fraud by those using EHRs and brainstorming among the panel members for possible fraud management solutions that could be built into EHRs. The panel divided into two groups: those developing recommendations that would be useful in preventing the commission of fraud and/or detecting fraud prior to payment of a claim, and a second group developing recommendations to assist in fraud detection after payment and assist in prosecution. Draft recommendations went through multiple iterations within the panel and a reduced set was made available for public comment. The public comments were subsequently reviewed in detail by the panel and recommendations were modified or eliminated as a result for the final report.

The original set of Guiding Principles received uniform praise and support from all segments of the healthcare industry. The recommendations for EHRs from the second report did not. Most of the public comments during the second contract regarding the EHR recommendations were supportive, but a substantial number raised concerns. Likewise, following the publication of the final report, there was support for most of the recommendations but a significant
amount of pushback on many of them. The difference in the
industry reactions to the two reports is not surprising. The
Guiding Principles of the first report were high level,
general, and somewhat like “motherhood” in nature. The
recommendations of the second report were specific, tough,
and would require significant actions on the part of the
healthcare IT industry that would compete with other
priorities. Pushback and debate is both healthy and expected.

The concerns raised about the EHR recommendations were
that they could violate consumer and physician privacy,
allow payers unwarranted access to electronic records, be
threatening to physicians regarding fraud investigation, add
cost to EHRs, and impede performance of EHRs. To the
extent that any of these is true, they are legitimate issues and
would have a negative impact on adoption of EHRs. The
expert panel took all of these potential issues into consider-
ation and crafted the final recommendations in a manner
which would either eliminate them or mitigate them to an
acceptable level commensurate with the problem. Nonethe-
less, there is room for continued debate and reworking of
the solution.

What is not an acceptable solution is to totally dismiss the
notion of building fraud management into EHRs as some are
advocating. Admittedly there is a cost to doing this and
there is some competition with other priorities. It became
clear during our interaction with both CCHIT and HITSP
that fraud management was not on either organization’s
radar screen. Although the leadership of both organizations
expressed support for dealing with the fraud problem, it
was also clear that neither organization had received any
mandate from the American Health Information Commu-

nity (or anyone else) to put it as a priority. Further, the
notion of requiring EHR vendors to implement functions
that would, in part, help payers or law enforcement agencies
to prosecute their customers would be not only be politically
incorrect for organizations that depend on vendor and
provider support but is perceived as conflicting with their
primary goal of promoting EHR adoption. EHR adoption is
an important goal, but we cannot have an attitude of EHR
adoption regardless of any potential negative consequenc-
es. Apparently, somewhere in the background of this
process, ONC or someone else in DHHS also became ner-
vous about being too visible about pushing fraud manage-
ment as a high priority. After our panel completed its work
and contributed to writing multiple drafts of our final
report, the report did get published under the title, “Recom-
dended Requirements for Enhancing Data Quality in Elec-
tronic Health Record Systems.”

That report title is not quite as misleading as it appears.
Although our entire process was focused on fraud manage-
ment, data quality of health records for patient care is
inseparable from the issue of fraud. Records that are com-
plete, accurate and medically appropriate are not fraudu-
lent. However, the fraud management piece requires ad-
titional metadata about the “who, what, when, and how” of
record completion in order to help sort out the minority bad
guys from the majority good guys. It is not a simple process
and the better the documentation, the easier it is to perform
a fraud management function. And, by the way, these same
metadata also protect the good guys from inappropriate
suspicion of fraud.

We have a problem. “We” means everyone: consumers,
payers, providers, and healthcare IT professionals. The sum
of $200B per year (or whatever is the true amount) is not
“chump change.” The fact that we don’t even know the true
amount is a problem. The fact that we don’t really know
how many of our providers commit fraud is a problem. The
best estimate of that number that I have been able to glean
from authorities in CMS who should know is that it is “less
than a majority.” We need to be more precise about that.
Whatever the current amount of fraud is, as stated earlier,
the widespread opinion is that without proactive fraud
management built into our IT infrastructure now, the prob-
lem will become significantly worse. After interacting with
people from CMS, the Office of the Inspector General and
officials in the Department of Justice, I have the distinct
impression that their view is that the healthcare IT commu-
nity does not take this problem seriously.

I interpret the reaction of the healthcare IT community
differently. We do take this problem seriously and no one
wants to see EHRs become facilitators of fraud. The concerns
expressed, however, especially the potential threat to EHR
adoption, are considered equally serious. I believe we can
turn this threat into an opportunity. The link between fraud
management and quality of records for patient care is real.
The improved security tools and increased metadata that are
required for fraud management are threats to the bad guys
and protection for the good guys. The opportunity is on the
financial side. Recent comments from the Director of the
Congressional Budget Office suggest that EHRs may not be
cost-effective and deserving of Federal investment.5 If we
can demonstrate that EHRs will make even a small dent in
the huge cost of healthcare fraud, this can become the major
financial justification for them.

In my view, the next steps need to bring all of the parties
together to work on this problem. Specifically, we need to
better quantify and characterize the current fraud problem
and better quantify and characterize the expected increase
with EHRs. This type of quantitative data was lacking in the
two ONC reports and is required not only to help convince
a skeptical healthcare IT community, but to better prioritize
and cost-justify the EHR functions required to mitigate the
problem. In the meantime, many of the recommendations
for EHRs are not controversial and we should implement
now these “low hanging fruit” recommendations for fraud
management. These include requirements for increased au-
dit information and protection of audit processes, use of the
National Provider Identifier in audit logs of provider input,
enforcement of strong user authentication, record modifi-
cation rules and tracking, improved output document track-
ing, increased security for electronic transmissions, and a
clear definition of the minimal requirements for the legal
EHR for business purposes.

In summary, the ONC contracts have succeeded in putting
fraud management on the table. It is our responsibility as
healthcare IT professionals to make sure it doesn’t get
tabled”.

References

1. National Health Care Anti-Fraud Association website. Available

