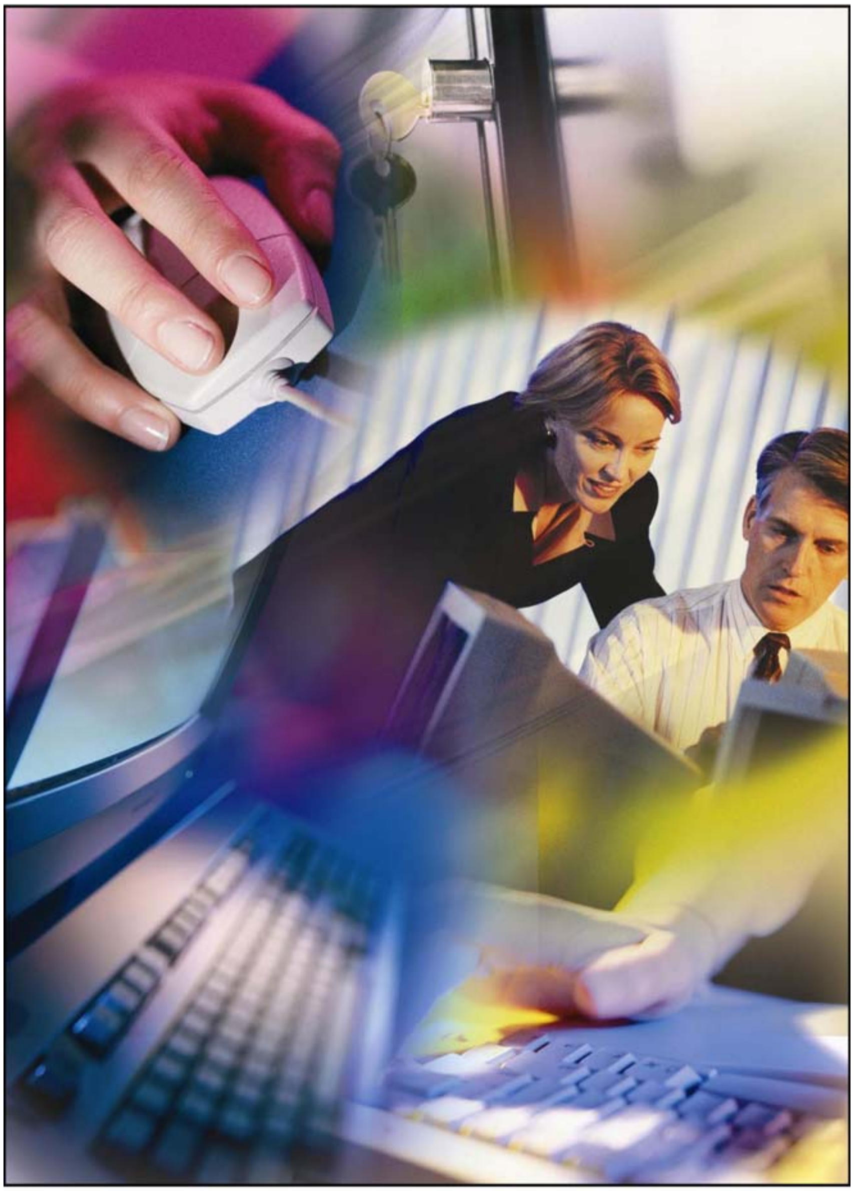


Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities

Prepared for:
The Office of the
National Coordinator,

U.S. Department of Health
and Human Services

Contract Number:
HHSP23320054100EC

September 30, 2005

Submitted by:

FORE
Foundation of Research
and Education of AHIMA

Foundation of Research and Education
American Health Information Management Association
233 North Michigan Avenue, Suite 2150; Chicago, Illinois 60601-5800
(312) 233-1100 ■ www.ahima.org

Contents

National Executive Committee Members

Co-Chairs

Arnold Milstein, MD, MPH, Medical Director, Pacific Business Group on Health and Chief Physician at Mercer Human Resource Consulting, San Francisco, CA

Donald W. Simborg, MD, Independent Consultant and Member, Joint Public Policy Committee of AMIA and AHIMA, Nevada City, CA

Committee Members

A. John Blair, III, MD, Chief Executive Officer, Taconic IPA, Fishkill, NY

Robert B. Burleigh, CHBME, President, Brandywine Healthcare Services, West Chester, PA

Rebecca S. Busch, RN, MBA, CCM, CBM, CHS-III, CFE, FHFMA, Chief Executive Officer and President, Medical Business Associates, Inc., Oakbrook, IL

Timothy J. Coleman, JD, Senior Counsel to Deputy Attorney General, U.S. Department of Justice, Washington, DC

Kenneth F. Faustine, Fraud Manager, Cigna, Hartford, CT

Donna Hoffmeier, Vice President, Government Affairs, Strategy and Policy for UnitedHealth Group, Washington, DC

Byron Hollis, Esq., CFE, AHFI, Managing Director, BCBSA National Anti Fraud Department

Richard Ingraham, Senior National Industry Strategist, SAS U.S. Commercial – Health & Life Sciences, Strategy, Alliance & Solution, Fort Collins, CO

Stephen L. Jones, DHA, Principal Deputy Assistant, U.S. Department of Defense Health Affairs, Washington, DC

Holly Louie, CHBME, BSN, Practice Management, Inc., Boise, ID

Jeff J. Matza, AHFI, CFE, Vice President, Special Investigations for Mutual of Omaha Company, Omaha, NE

Lewis Morris, JD, Chief Counsel to Inspector General, Office of Inspector General of the U. S. Department of Health and Human Services, Washington, DC

Maureen Mudron, JD, Washington Counsel, American Hospital Association, Washington, DC

Alison Rein, MS, Assistant Director of Food and Health Policy, National Consumers League, Washington, DC

Beth Schermer, JD, Partner, Coppersmith Gordon Schermer Owens & Nelson, Phoenix, AZ

James Speros, JD, Manager, Evaluation & Assessment Service, Office of Compliance & Business Integrity, Veterans Health Administration, Brecksville, OH

Jonathan Topodas, JD, Vice President and Counsel, Federal Government Relations, Law & Regulatory Affairs for Aetna, Inc., Hartford, CT

Jean de Traversay, Director of Healthcare Analytics, Fair Isaac Corporation, San Diego, CA

Susan Turney, MD, MS, FACP, CMPE, Executive Vice President and CEO, Wisconsin Medical Society, Madison, WI

Alan Yuspeh, JD, MBA, Senior Vice President, Hospital Corporation of America, Nashville, TN

Executive Committee Liaisons

Marsha Massey, JD, Affirmative Civil Enforcement Coordinator/Acting Health Care Fraud Coordinator, Executive Office for United States Attorneys, Washington, DC.

Steve Shandy, Fraud Section, Criminal Division, U.S. Department of Justice, Washington, DC.

Project Staff

Project Director

Susan P. Hanson, MBA, RHIA, FAHIMA
President, TerraStar Consulting Services, Nashua, NH

Senior Research Associate

Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS
President, Cassidy & Associates, Norcross, GA

Project Health Economist

Stephen T. Parente, PhD, MPH, MS
Principal, HIS Network, LLC, and Assistant Professor, Department of Finance, Carlson School of Management, University of Minnesota, Minneapolis, MN

Project Officer and Senior Advisor

Kathleen H. Fyffe, MHA
Office of the National Coordinator of Health Information Technology, U.S. Department of Health and Human Services, Washington, DC

Project Advisor and Expert

Richard W. Singerman, Ph.D.
Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, Washington, DC

FORE Representatives

Linda L. Kloss, MA, RHIA, Chief Executive Officer of the American Health Information Management Association, Chicago, IL

Eileen M. Murray, MM, CFRE, CAE, Vice President and Executive Director, Foundation of Research & Education, American Health Information Management Association, Chicago, IL

Executive Summary

Fraud has a significant impact on the U.S. health economy. The National Health Care Anti-Fraud Association (NHCAA) estimates that "...***of the nation's annual healthcare outlay at least 3% – or $51 billion in calendar year 2003*** was lost to outright fraud." Other estimates by government and law enforcement agencies place the loss as high as 10% of our annual expenditure, or $170 billion.[1] Fraud is a moving target and fraud control is highly dynamic. Although healthcare fraud is shifting to more sophisticated schemes that attempt to mask aberrant behavior patterns, fraud management can nonetheless reduce fraud's impact on healthcare costs. Throughout this report, the phrase "fraud management" is used to refer to the prevention, detection, and prosecution of healthcare fraud.

Fraud management is made all the more imperative by the federal prioritization of a Nationwide Health Information Network (NHIN). The prospect of a NHIN creates new challenges as well as new opportunities for fraud management. In January 2004, President George W. Bush called for widespread adoption of interoperable electronic health records (EHRs) within 10 years.

Toward that vision, President Bush signed Executive Order 13335 (EO), which directed the Secretary of the Department of Health and Human Services (HHS) to establish within the Office of the Secretary the position of National Coordinator for Health Information Technology (National Coordinator). The National Coordinator's responsibilities include coordinating federal HIT programs with those of relevant executive branch agencies, as well as coordinating with the private sector on its HIT efforts. On May 6, 2004, then Secretary Tommy G. Thompson appointed Dr. David J. Brailer to serve as the National Coordinator.

On July 21, 2004, the National Coordinator published "Framework for Strategic Action: The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care" (The Framework). The Framework outlined an approach toward nationwide implementation of interoperable EHRs and identified the following four major goals:

- Inform clinical practice by accelerating the use of EHRs.

- Interconnect clinicians so that they can exchange health information using advanced and secure electronic communication.

[1] *Healthcare Fraud: A Serious and Costly Reality for All Americans*, National Health Care Anti-fraud Association, http://www.nhcaa.org/pdf/all_about_hcf.pdf Site visited on August 14, 2005.

- Personalize care with consumer-based health records and better information for consumers.

- Improve public health through advanced bio-surveillance methods and streamlined collection of data for quality measurement and research.

On July 14, 2005, HHS Secretary Michael Leavitt announced the formation of a national collaboration, the American Health Information Community (AHIC), a public-private body formed pursuant to the Federal Advisory Committee Act. On September 9, 2005, Secretary Leavitt appointed 16 commissioners of the AHIC. The AHIC is to help transition the nation to EHRs in a smooth, market-led way. The expectations are that the AHIC will provide input and recommendations to the Secretary on the use of common standards and on how interoperability among EHRs can be achieved while ensuring that the privacy and security of those records are protected.

In April 2005, the Office of the National Coordinator for Health Information Technology (ONC) contracted with the Foundation of Research and Education (FORE) of the American Health Information Management Association (AHIMA) for two complementary projects. The objective of the first project, completed in June 2005, was to examine the state of automated coding software and its development and use to enhance anti-fraud activities.

The objective of this second project is to study how the use of health information technology (HIT) could enhance and expand fraud management. For this five month field-based research project, FORE convened a cross industry National Executive Committee to identify the best opportunities to strengthen the fraud management capability of a nationwide interoperable HIT infrastructure. The committee used literature review, cross industry site visits, and interviews to formulate its findings and recommendations. An economic impact model was developed using a Delphi technique and incorporating industry-accepted studies to project incremental impact of fraud management under several NHIN implementation scenarios.

The research findings from this project will inform the newly created American Health Information Community (AHIC) and provide guidance to the contractors awarded contracts resulting from the ONC RFPs described in the section in this document called “ONC Requests for Proposals.” These findings include invaluable lessons that have been learned from the banking and financial services (BFS) industries.

Many of the BFS fraud management program components are directly applicable to the healthcare industry. For instance, capabilities such as pattern recognition, system audits, and practice pattern monitoring are being employed with ever increasing effectiveness in BFS. The continuous evolution of healthcare fraud dictates the use of advanced analytics software to better detect fraud. Identification of potential vulnerabilities within these other industries will assist in the design of the NHIN infrastructure. However, because of the requirement to monitor fraud at a multitude of distinct levels, healthcare fraud management is more complex.

Field Research

The field research included formation of a National Executive Committee and associated workgroups,[2] development of an economic model, a literature review,[3] development of a structured data collection tool,[4] and public and private cross industry site visits and interviews.

The major findings that emerged from the field research were:

- "Fraud" in the healthcare context is defined by a number of legal authorities but all definitions have common elements: a false representation of fact or a failure to disclose a fact that is material to a healthcare transaction, along with some damage to another party that reasonably relies on the misrepresentation or failure to disclose.

- The healthcare fraud problem is a serious and growing nationwide crime, linked directly to the nation's ever-increasing annual healthcare outlay. In calendar year 2003, healthcare expenditures amounted to $1.7 trillion (the Office of the Actuary, Centers for Medicare & Medicaid Services). In that same year, it is estimated that losses due to fraud were 3-10% of the total amount of healthcare expenditures, or $51-170 billion.

- The healthcare industry is in a strikingly similar position to that of the financial services industry fifteen years ago. At that time, the banking industry began its transformation from paper to a sophisticated electronic environment. With a well thought out vision and strategy, banking addressed the inefficiencies of paper and invested heavily in the information technology infrastructure. Credit card fraud, estimated today to be less than 7 cents out of every 100 dollars, is widely perceived as a major problem. However, healthcare fraud is 100 times more costly!

- Technology can play a critical role in detecting fraud and abuse and it can help to pave the way toward prevention. While technology cannot eliminate the fraud problem, it can significantly minimize fraud and abuse and ultimately reduce healthcare fraud losses. The use of advanced analytics software built into the NHIN is critical to fraud loss reduction.

- Information available via the NHIN must comply with all federal and state laws. The federal government continues to expand its initiatives to uncover healthcare fraud, waste, and abuse. It is important that healthcare organizations have an effective compliance program in place. It is particularly important to develop a corporate culture that fosters ethical behavior. Many healthcare organizations are developing such a corporate culture through the adoption of corporate compliance programs.

[2] See National Executive Committee and Appendix D.

[3] The Bibliography includes both print and web references used in the literature review.

[4] See Appendix A.

- There is no single definition of the legal health record across the country. There is also no definition that encompasses the more complex electronic environment and various hybrid situations between paper and electronic records.

Economic Model

An economic framework of the costs and benefits of fraud management can shed light on the likely net impact of NHIN implementation on fraud. The principal research question for the economic framework is, “What are the expected fraud and non-fraud related costs/benefits associated with developing and implementing an NHIN with interoperable EHRs?”

The model examined four states through which the NHIN will evolve:

1. **The Status Quo as it is anticipated to be in 2006 after implementation of the Medicare Part D prescription benefit -** In this state, there is no NHIN. Some EHRs and electronic transactions such as e-prescribing exist but, with the exception of claims and prescription databases, there is little aggregate clinical data and no interoperability.

2. **Early NHIN** - In this state, electronic clinical transactions such as laboratory results and e-prescribing become widespread, EHR adoption increases, but there remains little EHR interoperability among providers.

3. **Intermediate NHIN** - This state features interoperability with intelligent coding tools. A record locator system exists to facilitate the interchange of clinical records among providers. Clinical vocabularies are in widespread use, ICD-10 has been implemented and intelligent coding tools are used for claims generation.

4. **Advanced NHIN** - This state features advanced analytics. Interoperability enables the aggregation of rich clinical and financial databases to which advanced analytic techniques are applied to detect patterns of fraud.

There are three major findings suggested from this analysis.

- There may be substantial savings in fraud-related expenditures that are possible from a move to an interoperable NHIN (State 3) that are not realized in the Status Quo and Early NHIN states.

- Moving to interoperability in State 3 may provide the most dramatic improvement in fraud net cost/benefit.

- The non-fraud related net benefits in States 3 and 4 are substantially higher than the fraud net benefits. That is, interoperability is projected to more than pay for itself regardless of its impact on fraud and abuse.

Results from this analysis should be interpreted with caution. The estimates presented are based on an economic impact model populated by the result of empirical studies and expert estimates of the costs of fraud prevention and health IT transition costs. However, many elements required expert estimation. At the very least, this analysis provides a structure for new evidence to be added so that areas where only expert opinion is available can be replaced with new empirical findings.

It is important to recognize, also, that the aggregate economic analysis undertaken here does not consider the actual distribution of these benefits and costs among the individual stakeholders involved. Benefits and costs will not be distributed evenly among all stakeholders.[5]

Guiding Principles and Recommendations

The ONC Anti-Fraud Project Executive Committee (the Executive Committee) was made up of 22 cross industry experts, including representatives of providers, payers, information technology, fraud investigative services, finance, and government. The composition of the committee was designed to bring together an expert panel reflecting a diversity of roles and perspectives. The Executive Committee convened in Washington, DC for two in-person meetings and convened three meetings via teleconference.

The Executive Committee members served on workgroups on each of the following topics: Guiding Principles; Economic Model; Fraud Management; Law Enforcement and Prosecution; and Information Technology and Infrastructure. The contributions of each workgroup resulted in Guiding Principles for that workgroup's area of focus. These essential guidelines were then integrated into the core Guiding Principles. Although broad consensus was achieved on the findings, principles, and recommendations presented in this report, the committee did not attempt to reach unanimous agreement on every view expressed.

[5] Libicki, M., Brahmakulam, I., *The Costs and Benefits of Moving to the ICD-10 Code Sets,* p. xvi. The RAND Corporation Science and Technology Institute, March 2004. http://www.rand.org/pubs/technical_reports/2004/RAND_TR132.pdf site visited on 8/14/2005.

The Executive Committee offers the Guiding Principles and associated recommendations presented in this report for AHIC's consideration as it begins the work of developing recommendations to HHS for achieving digital and interoperable health records within 10 years. The committee further recommends that additional work on healthcare fraud management be conducted and fully integrated with all other AHIC and ONC activities in FY 2006.

Preamble

The following Guiding Principles and Recommendations were developed by the National Executive Committee, a multi-stakeholder group of experts with significant experience and insight about the U.S. healthcare system, fraud management, health records, information management, and technologies. The principles are based on a solid understanding of the vulnerabilities of the system to individuals with the intent to defraud and of the opportunities that well-designed health IT offers. They are intended to guide policy makers and to support the needs of the vast majority of providers of services who are striving to comply with honesty to laws and requirements that affect billing and reimbursement. While many of the recommendations cannot currently be implemented, they identify the future technology, capability, and capacity that will be needed.

1. **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.**

   Recommendations:

   a. Develop enterprise management and operating policies for all stakeholders that will render the NHIN inherently resistant to fraud and support fraud management. Fraud management is defined as the prevention, detection, and prosecution of healthcare fraud.

   b. Build in as part of the NHIN infrastructure standards, procedures, and prototypes to facilitate nationwide healthcare fraud management.

   c. Certify electronic health record (EHR) software features and functions that are required or prohibited in the NHIN infrastructure to enable effective healthcare fraud management.

2. **EHRs and information available through the NHIN must fully comply with applicable federal and state laws and meet the requirements for reliability and admissibility of evidence.**

   Recommendations:

   a. Establish standards for the electronic maintenance, submission, and disclosure of health and financial information contained in the EHR. Standards should address accuracy, completeness, accountability, access and availability, audit ability (verifiability), identification, authentication, non-repudiation, integrity, digital certificate, digital signature, electronic signature, and public key infrastructure.

   b. Delineate data quality and electronic transmission standards.

c. Adopt a national approach to making public key infrastructure and other data security technologies available to all constituents of the NHIN.

d. Ensure that access to and disclosure of EHR content and other information available through the NHIN is consistent with health information privacy and security laws and other applicable laws.

3. **A standard minimum definition of a Legal Health Record (LHR) must be adopted for electronic health records (EHRs).**

   Recommendations:

   a. Establish national standards for the EHR to be maintained as a business record and, as such, adopt maintenance, retention, and disclosure practices for it as a business record that meets the requirements for reliable and admissible evidence.

   b. Establish national "EHR as the LHR" standards (using the current guidelines for paper health records as a generally accepted base) to address the transition from paper through hybrid to fully electronic health records.

4. **Comprehensive Healthcare Fraud Management programs must enable rather than inhibit nationwide EHR adoption.**

   Recommendations:

   a. Include fraud management features and functionality in the interoperable EHR without placing undue financial burden on the providers.

   b. Design EHR fraud management features that will not disrupt the provider workflow or interfere with the patient care process.

   c. Balance the development of fraud management programs on the NHIN with other priority interests and infrastructure design requirements, especially patient care.

5. **Healthcare Fraud Management is the responsibility of all healthcare stakeholders.**

   Recommendations:

   a. Disseminate definitions and guidelines to inform and address the impact and consequences of healthcare fraud on the economy, on patient health risk, and on population heath risk.

   b. Inform stakeholders of the interpretation of healthcare fraud guidelines with regard to EHR documentation and coding.

   c. Identify (consistent with current legal requirements) when and who has the right to access relevant portions of patient records (EHRs) through the customary mechanisms of the NHIN for the purpose of effective healthcare fraud management.

6. **Increased consumer awareness of healthcare fraud and the role health information technology and EHRs play in its reduction can improve the effectiveness of healthcare fraud management programs.**

   Recommendations:

   a. Develop and deploy a consumer awareness program on the role of information technology in healthcare fraud and its ability to detect and assist consumers to personally minimize fraud.

   b. Emphasize the benefits of the NHIN and EHRs in the national fight against healthcare fraud in program content and publications.

7. **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.**

   Recommendations:

   a. Mandate the minimum infrastructure necessary to ensure that EHR systems are maintained to facilitate ongoing fraud management programs and fraud prosecution activities.

   b. Define the EHR system requirements to support accurate documentation of the clinical care process, minimizing the potential to facilitate fraudulent practices.

   c. Develop NHIN IT infrastructure requirements to match or link the electronic documentation of a patient's clinical events and other relevant data files with the corresponding claims to enable healthcare fraud management.

   d. Develop minimum NHIN IT infrastructure procedures and requirements for data management, data efficiency, data exchange, data availability, security, backup, disaster recovery, record alteration, record authentication, and record retention that can be audited and verified.

8. **Standardized reference terminology and up to date classification systems that facilitate the automation of clinical coding are essential to the adoption of interoperable EHRs and the associated IT enabled healthcare fraud management programs.**

   Recommendations:

   a. Adopt uniform rules, regulations, and guidelines for standardized reference terminology and up to date classification systems across the country.

   b. Ensure that the organizations authorized to develop, deploy, and maintain such standards and guidelines assume ongoing responsibility to:

      - Provide clarity with a specific standard or guideline as required.

- Publish and disseminate the standards or guidelines in a manner that is generally understood.

- Respond in a timely manner to all requests for clarification of standards or guidelines.

c. Inform the individuals and entities choosing to participate in medical commerce that they are responsible for knowing and understanding the standards and guidelines with respect to clinical coding and classification.

9. **Fully integrate and implement fraud management programs and advanced analytics software in interoperable EHRs and the NHIN to achieve all of the estimated potential economic benefits.**

   Recommendations:

   a. Begin by building national work plans with specific timeframes for the varying levels of the NHIN's interoperability and its integration with and implementation of advanced analytics software for aggregate data analysis.

   b. Minimize the period of automated transactions without interoperability across providers.

   c. Move to a NHIN with analytic tools applied to aggregate data as quickly as possible once interoperability is achieved.

10. **Data required from the NHIN for monitoring fraud and abuse must be derived from its operations and not require additional data transactions.**

    Recommendations:

    a. Provide access to aggregate de-identified data generated in the normal operations of the NHIN, provided that the aggregation of data does not impose an obligation on the provider to generate data it would not otherwise have created for patient care.

    b. Assess the potential applicability of creating a Healthcare Information Sharing and Analysis Center (HISAC) as a component of a national fraud management program.

Conclusions

Healthcare fraud is a major weakness in the United States' healthcare system and it affects its ability to provide quality care and enhance patient safety. Escalating premium costs and the associated implications contribute to the need for conscious, urgent deployment of the NHIN with interoperable EHRs.

The need for portable health information has never been more evident than it is in the aftermath of the devastation to the Gulf coast by Hurricane Katrina in September 2005. Many of the paper based health records of patients in the affected areas were either destroyed or inaccessible, creating a void of medical information. A NHIN designed with fraud management requirements and interoperable EHRs would provide assurance against additional national financial losses due to fraud schemes following a national terrorist event or natural disaster.

Healthcare fraud hurts all stakeholders. The full extent of healthcare fraud is unknown, as there are no systematic measurements for fraud statistics, monitoring, or reporting. Fraud is dynamic and evolving and, as such, requires ongoing active surveillance using information technology and aggressive consumer involvement. Vigorous prosecution of healthcare fraud is a powerful deterrent to fraud perpetrators.

It is essential that fraud management programs be built into the NHIN infrastructure as part of its early design. Designing fraud management functionality into the NHIN has the potential to significantly reduce healthcare fraud losses. The interoperability between multiple EHRs is a major enabler of these loss reductions. Maximum benefit will be achieved by linking a claim with its corresponding documentation from an EHR, having the ability to access information in other EHRs regarding the same patient, and applying advanced analytics to aggregate clinical and financial databases. Without a deliberate effort to build fraud management into the NHIN, healthcare payers and consumers will be exposed to new and potentially increased vulnerability to electronically-enabled healthcare fraud.

The conventional thinking is that the adoption of EHRs and participation in an interoperable NHIN will be voluntary and not mandated. While there are certainly many understandable reasons for such an assumption, it is also apparent that those who are the most aggressive perpetrators of fraud will almost certainly opt out of the NHIN in order to avoid its anti-fraud capabilities. Thus, the architects of the NHIN and those involved with payment systems may want to consider the advantages and disadvantages of a system that at some point in the future might predicate payment of claims on participation in the NHIN, assuming of course that this becomes feasible technologically and economically. While such linkage would certainly increase the anti-fraud potential of the NHIN, strong consideration must be given to the fact that this might seem unduly coercive and could mandate significant added costs for certain providers.

National metrics for fraud management are required to systematically gauge and reduce healthcare fraud. Public and private stakeholder collaboration, as well as interstate cooperation, is also required to fight healthcare fraud. Such an anti-fraud enabled NHIN has the potential to identify emerging fraud schemes prior to payment. A shift from the current “pay and chase” fraud management programs to the proactive prevention of fraudulent claims prior to payment is made possible by interoperable EHRs and advanced analytics.

In conclusion, substantial savings in fraud-related expenditures would be enabled by an NHIN. It is important, however, to move quickly through the early transition state of the NHIN and achieve widespread adoption in order to maximize net savings.

Introduction

Fraud has a significant impact on the US health economy. The National Health Care Anti-Fraud Association (NHCAA) estimates that **"... of the nation's annual healthcare outlay at least 3% – or $51 billion in calendar year 2003"** was lost to outright fraud. Other estimates by government and law enforcement agencies place the loss as high as 10% of our annual expenditure or $170 billion."[6] Fraud is a moving target and fraud control is highly dynamic. Although healthcare fraud is shifting to more sophisticated schemes that attempt to mask aberrant behavior patterns, fraud management can nonetheless reduce fraud's impact on healthcare costs.

The continuous evolution of healthcare fraud dictates the use of advanced analytics software to better detect fraud. Fraud management is made all the more imperative by the federal prioritization of a Nationwide Health Information Network (NHIN). The prospect of a NHIN, however, creates new challenges as well as new opportunities for fraud management[7].

In April 2005, The Office of the National Coordinator for Health Information Technology (ONC) contracted with the Foundation of Research and Education (FORE) of the American Health Information Management Association (AHIMA) for two complementary projects.

The objective of the first project, completed in June 2005, was to examine the state of automated coding software and its development and use to enhance anti-fraud activities.

The objective of this second project is to study how the use of health information technology (HIT) could enhance and expand fraud management. The research findings from this project will inform the newly created American Health Information Community (AHIC) and provide guidance to the contractors awarded the ONC RFPs described in the section in this document called "ONC Requests for Proposals." For this five month field based research project, FORE convened a cross industry National Executive Committee to identify best practices to strengthen a nationwide interoperable HIT infrastructure. This field based research utilized literature review, cross industry site visits, and interviews to form its findings and recommendations. An economic impact model was developed using a Delphi technique and incorporating industry accepted studies that provided a first generation look at the costs and benefits for fraud detection and prevention via the NHIN.

[6] *Healthcare Fraud: A Serious and Costly Reality for All Americans*, National Health Care Anti-fraud Association, http://www.nhcaa.org/pdf/all_about_hcf.pdf visited on 8/14/05.

[7] For the purpose of this research, fraud management is defined as the prevention, detection, and prosecution of healthcare fraud.

Background and Context for this Project

This section provides background information about the creation of the Office of the National Coordinator for Health Information Technology (ONC), gives a synopsis of the recent Requests for Proposal (RFPs) released by ONC in June 2005, describes the Project's connection to the ONC RFPs, and summarizes Task 1 and Task 2.

Formation of ONC

On April 27, 2004, President George W. Bush signed Executive Order 13335 (EO) announcing his commitment to the development and nationwide implementation of an interoperable HIT infrastructure to improve efficiency, reduce medical errors, raise the quality of care, and provide better information for patients, physicians, and other healthcare providers. In particular, President Bush called for widespread adoption of EHRs within 10 years so that health information will follow patients throughout their care in a seamless and secure manner.

Toward that vision, the EO directed the Secretary of HHS to establish within the Office of the Secretary the position of National Coordinator for Health Information Technology (National Coordinator). The National Coordinator's responsibilities include coordinating federal HIT programs with those of relevant executive branch agencies, as well as coordinating with the private sector on its HIT efforts. On May 6, 2004, then Secretary Tommy G. Thompson appointed Dr. David J. Brailer to serve as the National Coordinator.

On July 21, 2004, the National Coordinator published "Framework for Strategic Action: The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care" (The Framework). The Framework outlined an approach toward nationwide implementation of interoperable EHRs and identified four major goals.

These goals are as follows:

- Inform clinical practice by accelerating the use of EHRs.
- Interconnect clinicians so that they can exchange health information using advanced and secure electronic communication.
- Personalize care with consumer-based health records and better information for consumers.
- Improve public health through advanced bio-surveillance methods and streamlined collection of data for quality measurement and research.

The Framework has enabled many industry segments, sectors, interest groups, and individuals to review how HIT could transform their activities, to consider how to take advantage of this change, and to participate in ongoing dialogue about forthcoming efforts.[8]

Building on these steps, two critical challenges to realizing the President's vision for HIT are being addressed: EHR adoption and interoperability. Interoperability using information technology is essential to achieve the industry transformation goals sought by the President.[9]

To address these challenges, HHS is focusing on several key actions: harmonizing health information standards; certifying HIT products to assure consistency with standards; addressing variations in privacy and security policies that might pose challenges to interoperability; developing an architecture for nationwide sharing of electronic health information; and conducting this project to explore and describe how the use of HIT can enhance and expand healthcare anti-fraud activities.

ONC Requests for Proposals (RFPs)

HHS has allocated $85 million to achieve these and other goals in FY 2005 and has requested $125 million in FY 2006. These efforts are interrelated and they will be coordinated through the formation of a new collaborative known as the American Health Information Community (AHIC).

On July 14, 2005, HHS Secretary Michael Leavitt formally announced the formation of a national collaboration, the AHIC, a public-private body formed pursuant to the Federal Advisory Committee Act. The AHIC was established to help smoothly transition the nation to EHRs. The AHIC is expected to provide input and recommendations to the Secretary on the use of common standards and on how interoperability among EHRs can be achieved while ensuring that the privacy and security of those records are protected.

In addition to the formation of the AHIC, the Office of the National Coordinator (ONC) issued four RFPs. The outputs of the contracts stemming from these RFPs will, in part, serve as inputs for the AHIC's consideration.

The RFPs focus on the following major areas:

Standards harmonization - To develop, prototype, and evaluate a process to harmonize industry-wide standards development and to unify and streamline maintenance and refinements of existing standards over time. Today, the standards-setting process is fragmented and lacks coordination, resulting in overlapping standards and gaps in standards that need to be filled.

[8] http://www.hhs.gov/healthit/frameworkchapters.html

[9] http://www.hhs.gov/healthit/frameworkchapters.html

Compliance certification - To develop, prototype, and evaluate a process to specify criteria for the functional requirements for health IT products.

Nationwide Health Information Network (NHIN) Architecture - To develop models and prototypes for a NHIN for widespread health information exchanges that can be used to test specialized network functions, security protections, and monitoring and to demonstrate the feasibility of scalable models across market settings.

Security and privacy - To assess variations in state laws and organization-level business policies around privacy and security practices, including variations in implementations of HIPAA privacy and security requirements that may pose challenges to automated health information exchange and interoperability.[10]

HHS established the AHIC and Secretary Leavitt appointed 16 commission members representing the public and private sectors. The AHIC will build on standardization both inside and outside the healthcare industry.

Specifically, the AHIC will perform the following functions:

- Make recommendations about how to maintain appropriate and effective privacy and security protections.
- Identify and make recommendations for prioritizing HIT achievements that will provide immediate benefits to consumers of healthcare (for example, national disaster prevention, preparedness, response and recovery; drug safety, lab results, bio-terrorism surveillance).
- Make recommendations regarding the ongoing harmonization of industry-wide HIT standards and a separate product certification and inspection process.
- Make recommendations for a nationwide architecture that uses the Internet to share health information in a secure and timely manner.
- Make recommendations about how the AHIC can be succeeded by a private-sector health information community initiative within five years.

Healthcare Anti-Fraud Study

In addition to these four RFPs, the ONC also commissioned this Healthcare Anti-Fraud Study (*Task Order HHSP23320054100EC)*. This project was undertaken to determine how automated healthcare coding software, a nationwide interoperable HIT infrastructure, and the use of EHRs will impact healthcare fraud issues.

Using President Bush's call for action as a springboard, the Project's primary and significant findings will inform the AHIC and provide guidance to HHS contractors. The

[10] http://waysandmeans.house.gov/hearings.asp?formmode=view&id=2944
Statement of David Brailer, M.D., Ph.D., National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. Testimony Before the Subcommittee on Health of the House Committee on Ways and Means, July 27, 2005.

Guiding Principles and Recommendations described later in this report apply to all four of the RFPs. The Project's findings will also be useful to other public and private initiatives that are working to advance health IT and fraud management and to organizations that are working on these goals.

It is essential that fraud management requirements be integrated with the design of the NHIN infrastructure. The Project's Guiding Principles and Recommendations provide a roadmap for AHIC and others to ensure that the NHIN's design will promote anti-fraud activities.

Introducing IT in the healthcare industry facilitates quality improvement and simultaneous cost reduction. "HIT is transforming how healthcare is delivered and it could allow a market to develop that would reward innovations in care delivery, make the healthcare system more responsive to consumers, and involve consumers much more actively in their own health and healthcare."[11]

Summary of Task 1 and Task 2

The purpose of the Health Information Technology and Healthcare Anti-Fraud Program Support Services Project (the Project) was to explore and describe how the use of HIT can enhance and expand healthcare anti-fraud activities. The project included two major Tasks.

Task 1 was a two-month descriptive study to

- Identify the characteristics of automated coding systems that have the potential to detect improper coding.
- Identify the components of the coding process that have the potential to minimize improper or fraudulent coding practices when using automated coding and relate these components to the role of the electronic health record (EHR).
- Develop recommendations for software developers and users of coding products to maximize anti-fraud practices.

Task 1 was completed by conducting a descriptive research study addressing both the developer and user perspectives. Both perspectives were considered necessary in order to assess issues related to actual use of automated coding products, auditing and validation methodologies employed by users, the interface of automated coding products with other systems/applications (the EHR role), and the functionality or logic used in development of these products. Users included any entity that utilizes automated coding software to generate diagnostic and procedural codes, including providers, contract coding companies, and billing companies.

[11] http://waysandmeans.house.gov/hearings.asp?formmode=view&id=2944
Statement of David Brailer, M.D., Ph.D., National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. Testimony Before the Subcommittee on Health of the House Committee on Ways and Means, July 27, 2005.

Task 2, which is the subject of this report, was accomplished in five months. It was designed as field research to identify best practices to enhance the capabilities of a nationwide interoperable HIT infrastructure to assist in healthcare fraud detection, prevention, and prosecution. The final report of the Task 1 work was available for the Task 2 project team.

Field Research

This section presents a thorough analysis of the field research. In addition to the economic model, the field research included formation of an Executive Committee, a literature review,[12] development of a structured data collection tool,[13] public and private cross industry site visits and interviews, and formation of Executive Committee workgroups.

This section is organized into the following three parts:

Part 1 - Provides a background on healthcare fraud.

Part 2 - Describes the methods used to conduct the research.

Part 3 - Presents results organized according to the themes that emerged during the site visits and interviews.

Background on Healthcare Fraud

The term “health care fraud” refers to an expansive variety of sanctioned conduct that occurs within the broad scope of healthcare commerce. In addition to different types of fraud, there are also differing degrees of fraud, to which both private individuals and governmental entities can respond via a variety of remedies and sanctions. These remedies and sanctions can be criminal, civil, or administrative. The appropriate sanction or remedy for a particular case depends upon its specific facts. In many situations, the efficient access to clinical records via interoperable EHRs can be a powerful tool to address potentially fraudulent conduct.

Congress has defined criminal healthcare fraud in Title 18, United States Code (U.S.C.) s 1347 as "knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any healthcare benefit program or 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."[14] Healthcare fraud schemes also may violate various other federal criminal statutes for which charges

[12] The Bibliography includes both print and web references used in the literature review.

[13] See Appendix A.

[14] For criminal health care fraud**,** “knowingly” means that the act was done voluntarily and intentionally, not because of mistake or accident; “willfully” means that the act was committed voluntarily and purposefully, with the specific intent to do something the law forbids; that is to say with bad purpose either to disobey or disregard the law. *See, e.g.,* Pattern Jury Instructions, Criminal Cases, United States Fifth Circuit District Judges Association, 1997*.*

may be filed depending on the specific facts of each case.[15] In a criminal prosecution, the burden of proof for a conviction is “beyond a reasonable doubt.”

Under the civil False Claims Act, 31 U.S.C. §§ 3729-3733 (1988), any person who performs any of the following actions is liable to the United States Government for a civil penalty of not less than $ 5,500 and not more than $ 11,000, plus 3 times the amount of damages which the Government sustains because of the act of that person…” [16]

(1) Knowingly presents, or causes to be presented, to an officer or employee of the United States Government or a member of the Armed Forces of the United States a false or fraudulent claim for payment or approval;

(2) Knowingly makes, uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the Government;

(3) Conspires to defraud the Government by getting a false or fraudulent claim allowed or paid;

(4) Has possession, custody, or control of property or money used, or to be used, by the Government and, intending to defraud the Government or willfully to conceal the property, delivers, or causes to be delivered, less property than the amount for which the person receives a certificate or receipt;

(5) Authorizes to make or deliver a document certifying receipt of property used, or to be used, by the Government and, intending to defraud the Government, makes or delivers the receipt without completely knowing that the information on the receipt is true;

(6) Knowingly buys, or receives as a pledge of an obligation or debt, public property from an officer or employee of the Government, or a member of the Armed Forces, who lawfully may not sell or pledge the property; or

(7) Knowingly makes, uses, or causes to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the Government.

[15] Examples from Title 18 U.S.C. include: §1347: health care fraud; §669: theft or embezzlement in connection with health care; §1035: false statements relating to health care; §1518: obstruction of a federal health care fraud investigation; §371: conspiracy to commit fraud; §287: false claims; §1001: false statements; §201: bribery (or alternatively Title 42 U.S.C. §1320: kickbacks); §1956-57: money laundering; §1343: wire fraud; and §1341: mail fraud.

[16] For purposes of the False Claims Act, the terms "knowing" and "knowingly" mean that a person, with respect to information--
(1) has actual knowledge of the information;
(2) acts in deliberate ignorance of the truth or falsity of the information; or
(3) acts in reckless disregard of the truth or falsity of the information,
and no proof of specific intent to defraud is required.

Therefore, when civil healthcare fraud cases under the False Claims Act[17] are settled, the federal government generally recovers the amount of the federal loss as well as additional money in the form of multipliers and/or fines. The burden of proof for a civil False Claims Act case is a “preponderance of the evidence.”

Other statutory administrative remedies are found in the Civil Monetary Penalties Law, Title 42 U.S.C. § 1320a-7a, and the Program Fraud Civil Remedies Act, Title 31 U.S.C. §§ 3801-3812. In addition, administrative remedies possessed by the HHS-OIG permit the exclusion of the provider from federal healthcare programs for a specified period of years (42 U.S.C. § 1320a-7b(f)); 42 U.S.C. § 1320a-7a; and 42 U.S.C. § 1320a-7(b)(7)).

The most common type of healthcare fraud involves a false statement, misrepresentation, or deliberate omission that is critical to the determination of benefits payable, or misrepresentation caused to be made that is material to entitlement or payment such as under the Medicare program. The violator may be a physician or other practitioner, a hospital or other institutional provider, a clinical laboratory or other supplier, an employee of any provider, a billing service, a beneficiary, a health plan employee, or any person in a position to file a claim for benefits.

Fraud schemes range from those perpetrated by individuals acting alone to broad-based activities by institutions or groups of individuals, sometimes employing sophisticated telemarketing and other promotional techniques to lure consumers into serving as the unwitting tools in their schemes. Seldom do perpetrators target only one insurer or either the public or private sector exclusively. Rather, most schemes are defrauding several private and public sector victims simultaneously.

Fraud can be detected and reduced through a variety of information technology capabilities, including abnormal pattern recognition, powerful system audits, practice pattern monitoring, and tracking of controlled substances. Other sectors of the economy, such as the credit card industry, have harnessed the power of technology to reduce fraud. “Credit card fraud has been reduced to about 7 cents out of every $100 spent on using cards.” Much of the success in detecting credit card fraud is attributed to technology’s effective recognition of spending patterns.[18]

[17] Title 31 U.S.C. §§ 3729-3733 (1988)

[18] *Signs of Fraud Go Beyond Signature, Credit Card Companies Use Artificial Intelligence to Thwart Thieves,* by Margaret Webb Pressler, Washington Post Staff Writer Sunday, July 21, 2002; Page H05

Methods

This project was directed at essentially new and rapidly evolving technology and policy. FORE convened a cross industry National Executive Committee to identify best practices to enhance the capabilities of a nationwide interoperable health information technology infrastructure to assist in healthcare fraud prevention, detection, and prosecution. This field based research also utilized literature review, cross industry site visits, and interviews to formulate its findings and recommendations. An economic impact model was developed — a first generation look at the cost/benefits for fraud detection and prevention on the NHIN.

The ONC appointed Kathleen H. Fyffe as the Project Officer and the FORE Foundation engaged the professional consulting services of Susan P. Hanson as the project director, Bonnie S. Cassidy as the project's senior research associate, and Stephen Parente, PhD as the Health Economist. Administrative support was hired, including a part-time editorial assistant and staff assistant.

The field-based research methodology consisted of the following major components:

Executive Committee

A national committee of 22 cross industry experts was appointed including representatives of providers, payers, information technology, fraud investigative services, finance, and government. This ONC Anti-Fraud Project Executive Committee (the Executive Committee) met in Washington, DC for two onsite meetings and convened three meetings via teleconference.[19]

Literature Review

Findings from the review were used to develop the data collection tool for the site visits and interviews with public and private cross industry experts in EHRs, payers/insurers, banking, financial services, advanced analytics technology, HIT infrastructure, federal agencies, providers, law enforcement, consumer affairs, claims clearinghouse, and others. Findings from the literature were used to formulate and validate the discussions associated with the Guiding Principles and Recommendations. Specific articles and reports were provided as orientation material to the Executive Committee.[20]

Site Visits and Interviews

Site visits, in person interviews, and telephone interviews were scheduled and conducted from May 9 through August 16, 2005. Telephone or in person interviews were conducted with approximately 117 individuals representing both the public and private sector. The interview method consisted of the project director and senior research

[19] See Appendix B for a complete list of committee members and their biographical summaries.

[20] See the Bibliography for a complete list of articles and other references provided to the Executive Committee

associate conducting the interviews utilizing a structured data collection instrument that was submitted to each interviewee prior to the scheduled meeting.[21]

Workgroups

Five working committees of the Executive Committee were established to focus on Guiding Principles and Recommendations related to five core areas of focus.

- Guiding principles
- Law enforcement and prosecution
- Fraud management
- Information technology infrastructure and implementation.
- Economic impact

The workgroup leaders presented their findings and deliverables to the onsite Executive Committee meeting that was convened on August 9, 2005. These Guiding Principles that call for comprehensive healthcare anti-fraud initiatives and fraud management programs are the outcome of the harmonization of the thought leadership of all workgroup participants.

Results

This section presents results organized according to the themes that emerged during the site visits and interviews.

The Healthcare Fraud Problem

There are many organized programs that perpetrate fraud and target the $1.7 trillion annual US healthcare claims. These fraud schemes include

- Providers submitting claims for phantom procedures.
- Billing for visits that never took place.
- Non-existent companies obtaining provider numbers and submitting claims for individuals who never received care.
- Companies submitting claims for durable medical equipment that was never received.
- Paying healthy citizens to come in for unnecessary visits.
- Providing unnecessary surgical procedures.

[21] See Appendix A for a list of the interview questions.

- Payment for services for claims with medical necessity certificates that were signed by a provider for a referral kickback.

- Fabricating claims from non-existent clinics.

- Non-professionals masquerading as healthcare professionals.

- Criminals buying real patient and provider information, submitting claims, and receiving payment for care that never happened.

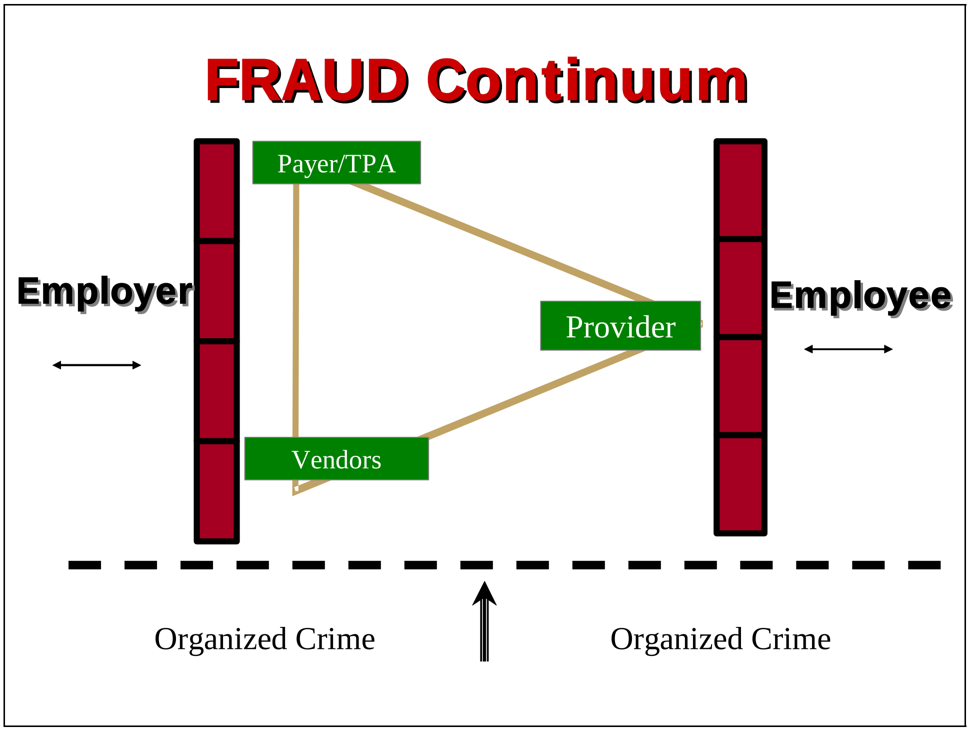
- Providers billing for more expensive services than those that were provided.

- Patients doctor-shopping or bouncing from one doctor to another in order to obtain multiple prescriptions for controlled substances.

- Patients alleging that non-medical procedures were medically justified and submitting claims for them.[22]

[22] http://www.ibx.com/pdfs/about_ibc/antifraud/fraud_top_ten.pdf

As depicted in the Fraud Continuum diagram,[23] schemes can be generated by each player within the brick walls and collusion is initiated among players outside the normal course of business (below the bottom line) to generate schemes on their fraud continuum.



Although a small percentage of healthcare stakeholders deliberately manipulate healthcare claims, healthcare fraud affects everyone. As a result, according to Oxford Health Plans, employers pay higher health insurance premiums for their employees and members pay more for healthcare benefits. Increasing costs of healthcare may also limit the level of care available to members from their healthcare providers.[24]

Fraud has experienced an explosive growth in some regions of the country - south Florida and Los Angeles are prime examples. Many have made fraud the criminal career path of choice for fraudsters looking to reduce risk while increasing returns. Entrepreneurial criminals actually are abandoning drug trafficking or more dangerous activities to enter the safe but lucrative arena of healthcare fraud.[25]

Prescription drug plans are expected to be the new target for healthcare fraudsters. In November 2005, an expected 29 million people 65 and older will start enrolling in

[23] Reprinted with permission from Rebecca Busch, CEO and President, MBA News, Inc.

[24] https://www.oxhp.com/main/fraud/affects.html United Healthcare, Oxford Benefit Management.

[25] Freeh, Louis J., Director, Federal Bureau of Investigation, Statement before the Special Committee on Aging, U.S. Senate, Washington, D.C., March 21, 1995, 2., Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow

Medicare's fully launched prescription drug insurance plan, costing an estimated $720 billion over the first decade. Prescription drugs are especially vulnerable to fraud, waste, and abuse.[26]

Estimates of the Fraud Problem and Efforts to Control It

Since the early 1990s, healthcare fraud has been viewed as a serious and growing nationwide crime, linked directly to the nation's ever-growing annual healthcare outlay, which in calendar year 2003 alone amounted to $1.7 trillion (the Office of the Actuary, Centers for Medicare and Medicaid Services). This represents a 7.7% growth in healthcare fraud over the prior year of 2002. Although fraudulent transactions constitute only a small fraction of the 4 billion health insurance transaction processed in the United States annually, those fraudulent claims carry a very high price tag.

"Estimates of annual losses to fraud range from 3% to 10% of national healthcare expenditures. This translates to $51 billion to $170 billion based on 2004 expenditures of $1.794 trillion. In comparison, credit card fraud, which is perceived as a huge problem, amounts to only $788 million in annual losses."[27] Healthcare fraud costs the public 100 times that of credit card fraud.

"CMS projects national health expenditures to reach $3.6 trillion in 2014, growing at an average annual rate of 7.1 percent during the forecast period from 2003 to 2014. As a share of gross domestic product (GDP), health spending is projected to reach 18.7 percent by 2014, up from its 2003 level of 15.3 percent. One of the most significant events impacting the projections is the new Medicare Part D prescription drug benefit mandated in the Medicare Modernization Act. The prescription drug benefit will take effect in January 2006."[28] Thus, it is not surprising that criminals view healthcare fraud as a lucrative field for illicit profit.

Since healthcare fraud may cost taxpayers as much as $170 billion a year, federal and state agencies have made healthcare fraud prosecution a primary focus. In 2001, the federal government won or negotiated more than $1.7 billion in judgments, settlements, and administrative impositions in healthcare fraud cases and proceedings. This is the largest return to the government since the inception of the Health Care Fraud and Abuse program established by the Healthcare Portability and Accountability Act of 1996. Yet, this return represents only a small fraction of the expected fraud losses. In addition, the number of healthcare fraud cases referred for criminal prosecution by HHS has significantly increased. Even following September 11, 2001, enforcing fraud and abuse remains a federal priority.

"The federal government concentrates its efforts to detect and prosecute healthcare fraud in its healthcare insurance programs, Medicare and Medicaid. Statutes enacted to

[26] Vardi, Nathan. June 20, 2005. *Prescription for Fraud*. Forbes Magazine

[27] http://www.bizintelligencepipeline.com/showArticle.jhtml?articleId=166402516 HSBC And SAS Building Advanced Card-Fraud-Detection System, by Steven Martin, Information Week, July 21, 2005.

[28] http://www.cms.hhs.gov/statistics/nhe/projections-2004/highlights.asp

deal with fraud in these specific programs have become necessities because Medicare, the government's second largest social program, continues to be an attractive target for fraud and abuse."[29]

Key fraud management themes identified during interviews with industry leaders are as follows:

- Build standardized and accepted management practices and processes aligned with the new technology.

- Encourage consumers to view their own billing information as one of the most powerful ways to deter fraud.

- Establish fraud management practices to prevent, detect, and prosecute healthcare fraud.

- Recognize the consumer role in assisting in the prevention, detection, and prosecution of healthcare fraud.

- Learn from advances and practices in the credit card and banking industries to prevent, detect, and prosecute fraud.

The private healthcare industry has committed resources to fraud prevention and recovery. According to the NHCAA's 2002 Anti-Fraud management Survey "the best anti-fraud efforts resulted in a paltry industry-wide $356 million in private healthcare fraudulent claims recovered or identified. That's less than four-tenths of 1%—little more than a drop in the bucket."[30]

[29] http://www.questia.com/PM.qst?a=o&d=5002005009, Health Care Fraud, Journal article by Jonathon Cone, Marisa Levinson, Shelley Finlayson, American Criminal Law Review, Vol. 40, 2003

[30] http://www.managedhealthcareexecutive.com/mhe/article/articleDetail.jsp?id=173378 Advanced analytics are a powerful secret weapon against healthcare fraud, August 1, 2005, Andrea Allmon, MD, Managed Healthcare Executive

Fraud Management: Process

Since 1992, when healthcare reform emerged as a matter of national debate, the issue of fraud management has received much attention. Unprecedented attention to the issue of healthcare fraud produced some successes.

There are three approaches to fraud management.

- The **Retrospective** approach identifies fraudulent claims *after* they have been adjudicated.
- The **Prospective** approach detects fraudulent claims *prior* to payment.
- The **Preventive** approach is a comprehensive approach that utilizes IT for ongoing pattern monitoring and analysis.

The most widely adopted approach to fraud and abuse detection is primarily retrospective in that business intelligence applications are applied against historical claims information. "Currently, 80% of fraud and abuse detection is performed using the retrospective approach. Retrospective systems are also valuable because they identify and store provider patterns and discrepancies. Payers report demonstrable return on investment from the use of retrospective fraud and abuse detection."[31]

Payers have the ability to stop the processing of fraudulent claims via the prospective approach, but are cautious to move toward a prospective claims review process. The reason for not wanting to implement automated prospective claims review processes is the fear of slowing down the payment process. "Many states have prompt pay laws requiring payment within a specified period after submission, with financial penalties for noncompliance. Even if payers migrate to prospective claims review, retrospective review will continue to be an effective and strategic tool for fraud and abuse detection."[32]

A comprehensive fraud management program is considered good business for any organization involved in the healthcare payment process. Information technology and systems provide the features and functions for fraud detection and recovery. "By 2007, healthcare payer organizations that adopt automated systems for fraud and abuse detection will see a return on investment of at least 5 to 1."[33]

A significant investment has not been made in adequate fraud management tools at the federal level because program administration costs are budgeted separately from program costs (that is, claims paid). This budgetary separation makes it virtually

[31] http://www.managedhealthcareexecutive.com/mhe/article/articleDetail.jsp?id=96834 Fraud and abuse applications pique payers' interests, Joanne Galimi, Managed Healthcare Executive, May 2004

[32] http://www.managedhealthcareexecutive.com/mhe/article/articleDetail.jsp?id=96834 Fraud and abuse applications pique payers' interests, Joanne Galimi, Managed Healthcare Executive, May 2004

[33] thttp://www.managedhealthcareexecutive.com/mhe/article/articleDetail.jsp?id=96834 Fraud and abuse applications pique payers' interests, Joanne Galimi, Managed Healthcare Executive, May 2004

impossible to consider the notion of "return on investment" in allocating resources for fraud management.[34]

Despite the level of political, legislative, and administrative attention paid to the fraud issue in the last several years, effective fraud management in the healthcare industry will be enabled only with the introduction of an interoperable EHR that would contain both clinical and financial records.

"When payers succeed in cracking down on fraud, everyone wins. The system runs more smoothly and efficiently and the cost savings to payers enable more affordable coverage plans and reduce costs to employers while improving quality of care. While advanced analytic tools have been used successfully for years in disease management, healthcare organizations are now finding them equally useful in claims processing and fraud detection. In an industry with as much as $170 billion a year lost to fraud and abuse, it's high time for healthcare organizations to study the potential impact advanced decision support systems may have on their bottom line."[35]

Key elements of a fraud management compliance program may include the establishment of an organizational structure including committees, preparing a fraud management compliance plan, recruiting and hiring fraud management executives and staff, instituting an internal hotline, providing compliance education and training, and ongoing quality assessment, auditing and process improvement for the program.[36]

Many instances of healthcare fraud suggest that existing control systems do not work the way we imagine they should. Often the manner in which schemes are revealed suggests detection is more luck than system. General Accounting Office (GAO) testimony to Congress has cataloged instances of fraud in the Medicare and Medicaid programs that, according to GAO, ought clearly to have been detected and stopped. But in each case the schemes came to light only through tip-offs or whistleblowers, rather than through the operation of routine monitoring or data mining.

The healthcare industry is uniquely differentiated from other fraud management environments because of the lack of metrics for ongoing measurement. According to Dr. Sparrow, there is a failure to systematically and routinely measure the scope of fraud in business and healthcare. "Measurement of fraud losses is quite feasible; it would involve standard sampling techniques backed by rigorous claims audits involving external validation procedures. Success with such techniques has been demonstrated

[34] Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow

[35] http://www.managedhealthcareexecutive.com/mhe/article/articleDetail.jsp?id=173378 Advanced analytics are a powerful secret weapon against healthcare fraud, August 1, 2005, Andrea Allmon, MD, Managed Healthcare Executive

[36]Lovitky, Jeffrey and Ahern, Jack, *Designing compliance programs that foster ethical behavior,* Healthcare Financial Management, March, 1999

by the Internal Revenue Service in its efforts to measure and control fraudulent claims for tax refunds based on the earned income tax credit."[37]

The ongoing lack of fraud control continues regardless of the level of political, legislative and administrative attention.[38] "An example of this was the recent discovery by the New York Times that the New York State Medicaid program has been misspending billions of dollars annually because of fraud, waste, and profiteering. A computer analysis of several million records obtained under the state Freedom of Information Law revealed numerous indications of fraud and abuse that the state had never looked into. New York State's Medicaid program has become a $44.5 billion target for the unscrupulous and the opportunistic."[39]

"Complex reimbursement methodologies, heterogeneous IT environments, and sheer claim volume are putting healthcare payer organizations at increasing risk of inappropriate claims payments because of fraudulent and abusive billing practices. Many payers have manual processes to help detect fraudulent claims. However, without an automated system it can take days to examine several legacy databases. The need to increase the speed and tenacity of fraud and abuse detection to help protect the organization from over billing, duplicate billing, and other fraud schemes that are difficult to detect manually is critical."[40]

The following factors are lessons learned from the article entitled "*Fraud Control in the Healthcare Industry: Assessing the State of the Art*" by Dr. Malcolm Sparrow.[41] These findings largely explain what makes fraud management, in any environment, such a difficult and complex challenge:

- What you see as the real problem never really is the problem. Most white collar frauds fall into the category of "non-self revealing" offenses. In fact, they will probably remain invisible forever.

- Industry standard performance indicators do not exist. The performance indicators that are available today are ambiguous, misleading, and not clear. If the amount of detected fraud increases, either the detection apparatus improved or the underlying incidence of fraud increased.

[37] Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow

[38] Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow

[39] Levy, Clifford and Luo, Michael, New York Medicaid Fraud May Reach Into Billions. New York Times, July 18, 2005

[40] http://www.managedhealthcareexecutive.com/mhe/article/articleDetail

[41] Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow, PhD

- Fraud management programs are viewed as a deterrent to productivity and service, as well as a threat to limited manpower. There is a fear that claims processing will be slowed down when a layer of fraud controls is implemented.[42]

- Bureaucracies have the tendency to establish pre-determined monetary returns instead of longer term, uncertain ones. As a result, efficiency usually wins the battle for limited resources.[43]

- "Like chess, fraud control is a dynamic game, not a static one. Fraud control is played against opponents who are smart, think creatively, adapt continuously, and enjoy creating complex winning strategies. A set of fraud controls that are perfect today, therefore, may be of no use tomorrow. Maintaining effective fraud controls demands continuous assessment of emerging fraud trends and constant, rapid revisions of controls."[44]

- Reliance is often placed on traditional enforcement approaches. The strength of the deterrent effect depends on the probability of getting caught, the probability of being convicted once caught, and the severity of the punishment once convicted. All three of these are notoriously low.

- The outcome of new fraud management programs is unknown. A risk is that a false optimism is created based on the hope that elimination of the types of scams most recently seen will mean elimination of the fraud problem. This fails to take into account the adaptability of the opponents, who take only a few days or weeks, at most, to change tactics once they are thwarted.[45]

Lessons From Other Industries

The field research for this HHS ONC Anti-Fraud and Health IT research project consisted of personal interviews, group interviews, site visits, and telephone interviews with representatives from financial institutions representing the credit card industry.

Interviews with representatives of the Financial Services Information Sharing and Analysis Center (ISACs) and Financial Services Round Table provided the following information:

- "In more than 1,000 identity theft cases, 70% were traced to inside data theft."[46]

- "84% of high-cost security incidents occur when insiders send confidential data outside the company."[47]

[42] Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow, PhD

[43] Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow, PhD

[44] Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow, PhD

[45] Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow, PhD

[46] Study conducted by the director of identity theft program at Michigan State University

- "One of every 500 outbound e-mails contains confidential customer, employee, or financial data; intellectual property; or competitive information."[48]

- 95% of data loss incidents are unintentional.

- Checking prevention technologies and management practices are necessary components of the banking and financial services (BFS) industry's fraud management programs.

- There is an increased need for transformation of knowledge workers in fraud management to be informaticists and analytics experts.

- Fraud is not a competitive issue. All organizations must collaborate and harmonize the data standards.

- Aggressive management of identity theft has reduced BFS fraud losses.

- Consumer involvement is critical.

- Credit card authentication is a model for EHR authentication.

The banking industry's transformation from paper-based information to electronic information began 15 years ago, when banking began addressing the inefficiencies of paper. Eight years ago, federal mandate opened up interstate banking laws and ushered in the IT era for banking.

It has taken banking 8 years to achieve a 51% rate of checks being electronic vs. paper. Banking made a huge investment in technology early to achieve efficiencies and fraud reduction. The banking industry required a national, uniform, standard coding system for banking transactions. The Banking Administration Institute (BAI) was created and made responsible for maintenance of quality standards and codes. Every standard bank transaction has an industry standard BAI code that allows for data sharing and that is used to detect fraud via advanced analytics software.

Check fraud is one of the largest challenges facing businesses and financial institutions today. With the advancement of computer technology, it is increasingly easy for criminals, either independently or in organized crime, to manipulate checks in such a way as to deceive innocent victims expecting value in exchange for their money.

A significant amount of check fraud is due to counterfeiting through desktop publishing and copying to create or duplicate an actual financial document, as well as chemical alteration, which consists of removing some or all of the information and manipulating it to the benefit of the criminal. Victims include financial institutions, businesses that accept bogus checks, and the consumer. In most cases, these crimes begin with the theft of a financial document. Check fraud can be perpetrated as easily as someone stealing a

[47] Gartner Report. Gartner: Deploy Detection Technologies to Cut Insurance Fraud and Abuse Joanne Galimi, Annemarie Earley, Publication Date: 20 April 2005 ID Number: G00127061

[48] Vontu's risk assessment studies

blank check from a home or vehicle during a burglary, searching for a cancelled or old check in the trash, or removing a check that was mailed to pay a bill from the mailbox.[49]

Invaluable lessons have been learned from the BFS industries. Many of the BFS fraud management program components are directly applicable to the healthcare industry. For instance, capabilities such as pattern recognition, system audits, practice pattern monitoring, and tracking of controlled substances are being employed by BFS with ever increasing effectiveness. However, because of the requirement to monitor fraud at a multitude of distinct levels, healthcare fraud management is more complex. Identification of potential vulnerabilities within the banking and financial services industries will assist in the design of the NHIN infrastructure.

Role of Technology in Healthcare Fraud Management

The utilization of fraud and abuse detection applications has many advantages. Automated applications for claims review is more efficient than a manual process, which enables payers to optimize the performance of the workforce. Software applications for fraud detection that utilize sophisticated data sensing can alert payers to new processes used to perpetuate fraud and abuse that otherwise may go undetected.

Credit card companies have been utilizing IT for real time fraud management. HIPAA will facilitate the ease with which software programs can conduct electronic reviews because the standardization of electronic claims mandated by its transactions and code set provisions somewhat enhance the uniformity of claims data.[50]

One of the challenges of IT adoption for fraud management is the resource intense process of mapping claims data from several databases to a central data repository. An ongoing challenge in the industry is what to do with the claims data once fraud and abuse detection cases have been identified. Determining which cases are likely to lead to recovery of funds and are worth taking action on is among the issues responsible for the slow adoption of fraud management programs.[51]

Technology can play a critical role in detecting fraud and abuse and can help pave the way toward prevention. Of course, technology cannot entirely eliminate the fraud problem. However, it can significantly minimize fraud and abuse, and ultimately help improve the bottom line. Insurance fraud will continue to outrun technological solutions.

"Through 2007, deployment of insurance fraud-detection technologies will not keep pace with opportunistic perpetrators of fraud (0.8 probabilities). During the past few years, Type A (technically aggressive and well-funded) healthcare payer organizations (payers) have been actively implementing automated fraud and abuse detection solutions. Type B (mainstream IT users with adequate funding) payers are now beginning to follow and adopt automated technologies for fraud and abuse detection. Beginning in 2005,

[49] http://www.ckfraud.org/ckfraud.html

[50] http://www.managedhealthcareexecutive.com/mhe/article/articleDetail

[51] http://www.managedhealthcareexecutive.com/mhe/article/articleDetail Fraud and abuse applications pique payers' interests, Joanne Galimi, Managed Healthcare Executive, May 2004

property and casualty (P&C) insurers that are Type A companies will take the lead in using technology to assign claims to the most appropriate resource and to prevent fraudulent claims. Gartner believes that this development will spur vendors to promote fraud-detection products to other types of insurers."[52]

The biggest opportunity to defray losses is likely to be the adoption of claim fraud-detection tools. As insurers increasingly move to decrease risks and losses, the industry anticipates revitalization and focus on claim processing, including fraud-detection technologies.

According to the April 2005 Gartner report, the following list describes technologies that aid in fraud and abuse detection:

Internal database comparisons -These technologies compare internal databases to aggregate data to detect anomalies and investigate historical internal data for multiple claims activity. For example, database comparison can uncover insured surname or address spelling errors that are suspicious, or an underwriter's claim history that warrants closer inspection.

Internal/external database comparisons - By combining internal and external databases, insurers can access historical claim experiences from many perspectives. External databases provide extra data, such as automobile vehicle records, to assess the experience of multiple providers and non-insurance sources.

Pattern recognition - By integrating a wide variety of data sources, insurers can compare analyses of customary claim experience and repeatable fraudulent patterns against current claim information. Pattern recognition is used in conjunction with claim experiences, such as in workers' compensation claims, to determine whether the experience level of most insurers for a type of injury is in pattern with the insurer's claim.

Voice stress analysis - By detecting slight inaudible fluctuations in the human voice and measuring "micro tremors" to identify words delivered under stress, insurers can evaluate potentially inaccurate information. Cognitive interviewing techniques usually accompany voice stress technology to help identify and separate fraudulent information from honest responses. Several U.K. insurers have successfully piloted this technology.

Predictive and statistical analytics - Use of these tools exposes multiple access points and databases to rigorous algorithms to predict and link data into meaningful segmentation and clustering for evaluation and scoring. Fraud scoring helps claim agents to distinguish suspicious or fraudulent claims from normal claim activity. Advanced neural networks, decision trees, self-organizing maps, and algorithms that provide segmentation and cluster analysis to identify fraud comprise predictive modeling technologies.[53]

[52] Gartner: Deploy Detection Technologies to Cut Insurance Fraud and Abuse Joanne Galimi, Annemarie Earley, Publication Date: 20 April 2005 ID Number: G00127061

[53] Gartner: Deploy Detection Technologies to Cut Insurance Fraud and Abuse Joanne Galimi, Annemarie Earley, Publication Date: 20 April 2005 ID Number: G00127061

Some types of fraud will be enabled by the use of EHRs. Effective fraud control requires unpredictability and mystery. The perpetrator of fraud must feel some element of the risk of random review in order to be deterred. Fully automated systems can be consistent in outcome and randomized in application. This is an objective for fraud management systems.

Some of the thought leadership on the role of technology pertaining to the EHR and fraud management includes the following:

- There must be some minimum level of IT infrastructure present to ensure that EHRs can be protected and preserved for purposes of fraud and abuse prevention, detection, and prosecution.
- The matching or coupling of the clinical record and the financial record/claim is vital, particularly for considering the appropriateness of care for a given condition as well as fraud management.
- Weak links in the movement of information between provider, patient, payer, and employer must be strengthened.
- Weak links in anti-fraud software, education, and compliance practices today must be corrected.

Barriers to Healthcare Fraud Management

There is no single definition of the legal health record across the country. According to a summary published in June 2005 by ONC, there is a need for additional and better-refined standards; addressing privacy concerns; paying for the development and operation of, and access to the NHIN; accurately matching patients; and addressing discordant state laws regarding health information exchange.

The standardization of health records is inhibited by the lack of uniformity of laws and regulations among the states. Content of health records varies from provider to provider. State laws and regulations differ regarding record content and format. Some do not permit electronic formats. These differences should be analyzed during the course of creating a NHIN or network of interoperable EHRs.[54]

For an EHR system to be successful, patients must trust that their information will be held confidential. For this reason, adequate protection for the privacy of health information included in the system is essential in the development of health information networks. As DHHS concluded, “the entire health delivery system is built upon the willingness of individuals to share the most intimate details of their lives with their health providers.”[55]

[54] American Health Lawyers Association, The Quest for Interoperable Health Records: A Guide to the Legal Issues Establishing Health Information Networks

[55] 65 Fed. Reg. 82,467 (Dec. 28, 2000).

While few states today have laws or regulations specifically addressing the security of electronic health records, such laws inevitably will be passed as EHRs become more common. For example, states may have laws regulating computer security, mandating security breach reporting, requiring specific steps for introduction into evidence, prohibiting or allowing electronic signatures in different situations, or combating identity theft.[56]

The federal government continues to expand its initiatives to uncover healthcare fraud, waste, and abuse. It is therefore more important than ever that those healthcare organizations have an effective compliance program in place. The organization should have a compliance officer with adequate authority and staff to carry out the compliance program's functions. The program should include an ethics code, an internal hotline that employees can use to report compliance concerns, and education and training for all employees. In addition, the program should be audited periodically to ensure its viability. To be successful, a compliance program also needs the support of the healthcare organization's senior management.

Given the federal government's current emphasis on combating fraud, waste, and abuse, healthcare organizations are finding it particularly important to develop a corporate culture that fosters ethical behavior. Many of these organizations are manifesting such a corporate culture through the adoption of a corporate compliance program.

The majority of literature reviewed indicates that fraud management efforts to control healthcare fraud don’t begin to touch the problem. In most organizations, the amount of fraud found in the system depends only on how hard one looks.[57]

[56] American Health Lawyers Association, The Quest for Interoperable Health Records: A Guide to the Legal Issues Establishing Health Information Networks

[57] Fraud Control in the Healthcare Industry: Assessing the State of the Art by Malcolm K. Sparrow

Economic Model

The NHIN will offer new opportunities to detect fraud as well as expose new areas of vulnerability for fraud. Information technology can both enable and detect fraud. If sufficient fraud detection and prevention opportunities can be identified by advancing from today's health IT infrastructure of largely standalone health insurer and medical providers systems to the interoperable system envisioned in the health IT strategic framework,[58] the benefits of advancing to the NHIN will outweigh the costs. An economic framework of the costs and benefits of fraud detection can shed light on the net value of the NHIN regarding fraud.

This section presents the first comprehensive estimates that tally the projected costs and benefits associated with fraud-related healthcare activities under future interoperable health IT infrastructure scenarios. The method used is a standard cost/benefit analysis where all known and identifiable impacts are relayed in monetary dollar units. The model applies the discipline of economics by recognizing that fraud is a non-recoverable cost to society that benefits neither the consumers nor the producers in a market economy.[59]

This section is organized into the following five parts:

Part 1 - Briefly discusses the principle research question and its rationale.

Part 2 - Describes the methods used to quantify the projected costs and benefits. Four states of the world are introduced for comparison purposes including: 1) Status Quo, 2) Early NHIN with non-interoperable EHRs, 3) Intermediate NHIN with intelligent coding tools and interoperability, and 4) Advanced NHIN with intelligent coding tools, interoperability, and analytic fraud tools.

Part 3 - Summarizes the results in each of the states based on the cost and benefit items as identified by the literature and an expert panel.

Part 4 - Discusses the implications of the economic model.

Part 5 - Offers several recommendations based on the implications and interpretation of the results.

[58] U.S. Department of Health and Human Services, "The Decade of Health Information Technology Delivering Consumer-centric and Information-rich Health Care," July 2004.

[59] Darby M. R., E. Karni, "Free Competition and the Optimal Amount of Fraud", *Journal of Law and Economics,* Vol. 16, No. 1:67-88, 1973

Principal Research Question

At present, the cost of healthcare fraud could be tens of billions of dollars.[60] Future efforts aimed at stemming healthcare fraud will need to prevent and detect the loss of resources due to fraud. The fraud management game is dynamic, not static. Maintaining effective fraud management tools demands the continuous assessment of emerging fraud trends and constant rapid revision of controls.[61] The creation of a new health IT infrastructure will increase the speed of transactions, both fraudulent and not. Therefore, it is prudent to examine projected costs and benefits of fraud detection and prevention under different future IT development scenarios.

As a result, the principal research question is:

> **What are the expected fraud/non-fraud related costs/benefits associated with developing and implementing a NHIN with interoperable EHRs?**

To answer this question, estimated fraud-related and non-fraud related costs and benefits were inventoried and tallied separately. Fraud-related costs include the current resources lost due to various types of fraud including identity theft, provider as well as patient, and the seeking of reimbursement for fake services. They also include the costs of detecting fraud. Fraud management-related benefits result from activities or technologies that enable either the prevention or recovery of healthcare monetary resources lost due to fraud. The magnitude of fraud-related costs and fraud management-related benefits varies depending upon the underlying IT infrastructure in place.

Since new methods of detecting fraud are dependent upon new technology platforms, the non-fraud related costs of those platforms, such as a NHIN, were considered separately. Of course, the NHIN produces non-fraud management-related benefits as well, thus those benefits were recorded and considered. By addressing both fraud-related and non-fraud related costs and fraud management-related and non fraud management-related benefits, a more complete assessment of the fraud, abuse, and prevention value of the NHIN was projected under each of the IT enabling scenarios.

[60] *Healthcare Fraud: A Serious and Costly Reality for All Americans*, National Health Care Anti-fraud Association, http://www.nhcaa.org/pdf/all_about_hcf.pdf site visited on 8/14/2005 site visited on 8/15/2005.

[61] Sparrow, M.K., *License to Steal: Why Fraud Plagues America's Health Care System,* Westview Press, Boulder, Colorado, 1996.

Methods

This section describes the methods used to quantify the projected costs and benefits.

Conceptual Model and Assumptions

The conceptual model for this analysis is straightforward. A consumer – and potential patient – derives a benefit from medical care through an improvement in the patient's health status. Fraud activities diminish the welfare of the consumer by either providing an additional cost (directly or indirectly) to patient care to cover the expense to the consumer or the consumer's insurer of an unneeded and possibly fictitious good or service. This serves as a definition of a fraud-related cost.

A fraud management-related benefit is the result of any activity that restores societal resources lost as a result of fraud. A fraud-related benefit is also defined as the result of any activity that prevents future fraud. This type of benefit may never be recoverable, but it nevertheless is what economists may consider an opportunity cost. In this case, fraud prevention foregoes the alternative of fraud creation. With respect to health IT, economists value the benefit derived from the increased use of EHRs from an opportunity cost perspective as well as a foregone cost of, for example, a medical error from a patient order entry system.

The methods used in this analysis are common within the context of medical technology evaluation studies where the costs and benefits of a new treatment are compared to that of a traditional therapy. As such, this method does not involve a formal economic model. Rather, it relies on economic principles of consumer welfare analysis and monetary valuation of the aforementioned opportunity costs following the approach outlined in the comprehensive review of the field by the Institute of Medicine.[62] This approach requires an inventory of the estimated costs and benefits of different technologies scaled to the level of citizen and then multiplied by the size of the potential population affected. In this case, the scope of the NHIN is truly societal so all of the results are in 2005 dollars expressed as national cost or benefit.

The approach was designed with future enhancement and adaptation in mind. Many of the cost and benefit items used are generated either from assumptions derived from actual health IT cost studies or expert opinion. As current and future research in health IT valuation increases, cost and benefit items in this model can be revised and updated. In future enhancements to this model, where the trajectory of NHIN scenarios is set to specific timetables with all stakeholders committing to firm milestones, this method can be used to develop a multi-year projection and describe the trajectory of costs and benefits. The approach used for this analysis assumes the annual costs of systems with annualized estimated transition costs amortized into the scenario by simply scaling any multi-year capital cost expenditure as an additional annual cost.[63]

[62] Gold, Marthe R. et al. *Cost-Effectiveness in Health and Medicine*. Oxford University Pres: New York, New York, 1996.

[63] As a starting point for this analysis, no discount factors are used because the growth and scale of the expenditures for an NHIN remains unknown is likely to be non-linear. Thus assuming a linear discount

Four States of the World

The analysis assumes four states of the world for fraud-related and non-fraud related cost and benefit comparison.

Each state is described as follows:

State 1 - Status Quo without a NHIN - This is the present state of the world in which health IT data systems are largely standalone systems owned by different stakeholders in the health economy and paper based medical records in physician practices. The principle health IT data generators in this world are medical providers[64] and public as well as private insurers. With the exception of integrated delivery systems, data resides in institution-specific silos, except for payment and prescription transactions. This world is assumed to include early use of e-prescribing due to Medicare Part D beginning in January 2006. With regard to fraud, e-prescribing presents a new vulnerability because of the increased velocity of authenticated automated transactions.

State 2 – Early NHIN with limited interoperability - This is a future state in which elements of an electronic health record, such as diagnostic testing results and e-prescribing, become widespread transactions between healthcare providers, insurers, and possibly consumers in consumer-directed health plans. There is increasing use of EHRs but interoperability is limited.

State 3 – Intermediate NHIN with interoperability and intelligent coding tools - In this state, a NHIN has been implemented with a record locator technology and the interchange of clinical data between provider systems. Also, intelligent coding tools are being used that provide a better context for the coding of a treatment or diagnosis. The NHIN is more likely to be using ICD-10 codes, which can more accurately document a person's true health disposition than ICD-9 codes. Though this will not prevent fraud outright, the 'gray area' fraud, where up-coding can represent a situation that exaggerates the severity of a patient's condition for provider financial gain, may be deterred somewhat.[65]

State 4 – Advanced NHIN with interoperability and analytic tools to detect fraud - This state builds on the previous state of an assumed NHIN infrastructure with new analytic tools to detect fraud. These tools are enabled by the ability to aggregate clinical data across interoperable EHRs. They will rely on algorithms that use record locater technology to verify patient outcomes based on a scan of all other data prior to payment. Record locator technology can also be used for random cyber audits where a certain set of cases is referred for investigation to identify possible fraud activities as a learning and adaptation exercise. The NHIN is a completely computerized system and, as such,

factor, for example, might produce results due more to speculative discounting than actual technology cost differences.

[64] Medical providers are defined generally as physicians, hospitals, pharmacists and other person or institution engaged in the delivery of heath services.

[65] Libicki, M., Brahmakulam, I., *The Costs and Benefits of Moving to the ICD-10 Code Sets,* p. xvi. The RAND Corporation Science and Technology Institute, March 2004. http://www.rand.org/pubs/technical_reports/2004/RAND_TR132.pdf site visited on 8/14/2005.

creates a concern that it will create predictability that can be exploited. Effective fraud management requires an advanced element of investigation assuming this new state of the world.[66] In this state, investigation will include advanced analysis of treatment patterns using the aggregated clinical data.

Costs and Benefits Inventory

Using these four states, an inventory of the anticipated costs and benefits associated with each one was compiled. This inventory is based on a review of the health IT literature and expert opinion available through the economic fraud working group and Executive Committee of this project. Once cost or benefit was identified, a monetary value was taken from either the clinical literature or expert opinion and scaled to a per US citizen value. A similar approach was used by Walker et al (2005) to estimate the net benefit of an interoperable health IT infrastructure.[67]

Descriptions of the types of costs and benefits identified include both fraud-related and non-fraud as follows:

Costs - fraud-related: These costs represent the most direct burden of fraud expenses in the healthcare system. They include the cost to detect and interdict fraud as well as the actual cost of the fraud. Many of the costs used are extrapolations from the HHS Office of Inspector General Semi-Annual Report (October 2003 – March 2004) and expert opinion of the workgroup.

These costs include

- Identity theft, defined as the use of someone’s identity for medical care services to which that person is not entitled under that person’s benefits.
- Billing for services that were never completed.
- Billing for services that were never completed under a real provider's ID.
- Unnecessary services performed for revenue generation only.
- Up-coding and misrepresentation of treatment.
- Medicare and Medicaid annual expenditures on fraud detection and prosecution.
- Private sector annual expenditures on fraud detection and prosecution.
- Costs of intelligent tools to gather data from the EHR.

[66] Sparrow, M.K., *License to Steal: Why Fraud Plagues America’s Health Care System,* Westview Press, Boulder, Colorado, 1996

[67] Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W., Blackford, M., *The Value of Health Care Information Exchange and Interoperability,* Health Affairs Web Exclusive, January 2005.

- Costs of fraud detection analytic tools.

Costs - non-fraud related: These costs primarily represent the investments necessary to implement the various IT infrastructure states of the world. A recent article by Kaushal et al. (2005) provided much of the basis for the estimated annual and operating costs of a NHIN and other states of the world.[68]

These costs include

- Capital costs
  - Capital cost of physician IT investment on an annual basis.
  - Capital cost of hospital IT investment on an annual basis.
  - Capital cost of other provider (SNF, pharmacy) IT investment on an annual basis.
- Operating costs
  - Operating cost of physician IT investment on an annual basis.
  - Operating cost of hospital IT investment on an annual basis.
  - Operating cost of other provider (SNF, pharmacy) IT investment on an annual basis.
- Other costs, such as
  - Data storage costs for retention.
  - Physician transition interoperability capital costs.
  - Hospital transition interoperability capital costs.
  - Other provider transition interoperability capital costs.

Benefits – fraud management-related: The fraud management-related benefits of various IT platforms are associated with any recovery of fraudulent payments as well as the prevented or opportunity costs of fraud detection. These estimates are based on the OIG report (2004), the RAND analysis of ICD-9 to ICD-10 conversion and its net impact on fraud prevention, as well as expert opinion.

These benefits include

- Annual recovery of payments made by government for fraudulent claims.

[68] Kaushal, R., Blumenthal, D., Poon, E., Jha, A., Franz, C., Middleton, B., Glaser, J., Kuperman, G., Christino, M., , Fernandopulle, R., Newhouse, J., Bates, D.W., *The Costs of a National Health Information Network,* Annals of Internal Medicine, Vol. 143, No. 3, pp. 165-173, August 2, 2005.

- Annual recovery of payments made by the private sector for fraudulent claims.
- The net benefit of gaining more accurate depictions of disease and reducing the likelihood of fraudulent up-coding.
- The identification of new leads from the availability of more digital fingerprints.
- The verification and validation of actual services through phone call-back or Web-based services.
- Patient verification of services through the Web or through EHR portal.
- Digital verification of services rendered by actual patients and providers.
- Reduction in record assembly time by use of common identifier and increasing digital media.
- Automated digital authentication to authorize claims billing and payment.
- Real time verification of eligibility benefits and possibly real time debiting in the case of HSAs.
- Reduction in consumer time spent dealing with the consequences of fraudulent claims.

Benefits - non-fraud management-related: The argument for the societal benefits of an improved health IT infrastructure have been documented by the studies cited in the Institute of Medicine's *Crossing the Quality Chasm* (2001) report as well as the DHHS Strategic Health IT Framework (2004). To develop a counter balance to significant investment costs of a NHIN, the non-fraud related benefits are detailed. The sources for these estimates include the Walker et al. (2005) estimated savings from a NHIN,[69] studies documenting avoidable medical error where a NHIN may have an impact,[70] as well as expert opinion.

These benefits include

- Avoidance of duplicating laboratory and imaging tests.
- Avoidance of redundant information already available digitally.
- Less labor time to verify eligibility.
- Less material and labor time to service paper documentation.

[69] Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W., Blackford, M., *The Value of Health Care Information Exchange and Interoperability,* Health Affairs Web Exclusive, January 2005.

[70] Zhan, C., Miller, M. *Excess Length of Stay, Charges, and Mortality Attributable to Medical Injuries During Hospitalization*. JAMA 290(14) 1868-1874.

- Less time to store and retrieve paper records.

- Reduction in the time spent by a consumer in phone trees and recording unnecessary information (for example, every EOB must be opened).

- Reduction in societal medical cost and loss of life due to medication errors.

- Reduction in societal medical cost and loss of life due to clinical errors (for example, operating on the wrong leg).

- Reduction in societal medical cost of duplicate diagnostic tests.

- Reduction in societal medical cost of unneeded medical surgeries.

- Reduction in malpractice costs and legal fees due on a per case basis due to improvements in avoidable error.

- Reduction in additional physician costs associated with ER and avoided hospital services[71].

- Reduction in additional pharmacy costs associated with ER and avoided hospital services[72].

- Reduction in referral visits to screen future care provider through some screening from pay for performance (P4P) initiatives.

- Reduction in provider time, bundling, storing, and forwarding of records to patients, providers, and health plans.

Expected Change in Benefits and Costs under Different Scenarios

With an inventory of costs and benefits, both fraud-related and not, monetized for a societal annual impact, the estimated change was considered by expert opinion based on previous experience and expectations of the NHIN rollout. For example, there was a 100% change expected for the use of digital signatures to identify fraud under the Status Quo because it simply does not exist currently as a technology option. In the two NHIN states of the world, State 3 and State 4, the benefit associated is then seen as possible, but only to the fullest extent with the use of analytic tools.

States 3 and 4 in the project are recognized as the most subjective. As a result, several working rules were used to make the estimates shown later in this section. First, whenever possible, empirical evidence was sought. When it was not available, a conservative estimate was used and then discussed as appropriate. A second rule was that the difference between States 3 and 4 assumes that the operations in State 4 will be

[71] This is a benefit associated with inpatient cost savings reported in the literature, but not usually extended to consider associated physician and pharmacy costs in both the inpatient and outpatient settings.

[72] This is a benefit associated with inpatient cost savings reported in the literature, but not usually extended to consider associated physician and pharmacy costs in both the inpatient and outpatient settings.

the most advanced because of prior experience gained reaching the state, including new and unforeseen uses of the data that will not just benefit fraud detection, but also clinical improvements in efficiency and productivity.

A final rule was to minimize double-counting benefits that are closely related. As a result, more granularity was used to identify and quantify benefits in order to disentangle the overlap. If overlap proved inevitable, expected changes were made more conservatively between the two correlated benefits.

Results

This section summarizes the results in each of the states based on the cost and benefit items as identified by the literature and an expert panel.

Table 1 - Fraud-Related Annual Costs

Table 1 presents data indicating that the healthcare industry is vulnerable to fraud and perpetrators of fraud will continue to attempt to outwit the system regardless of the fraud management and detection tools being used. The dramatic fraud-related costs in the Status Quo and Early EHR states are the inevitable result of the increasing predictability of electronic claims processing[73] coupled with the lack of the intelligent and analytic components of State 3 and State 4 that would make claims submitted and paid electronically safer.[74] States 1 and 2 both assume the increased costs of fraud related to the new Part D prescription benefit.

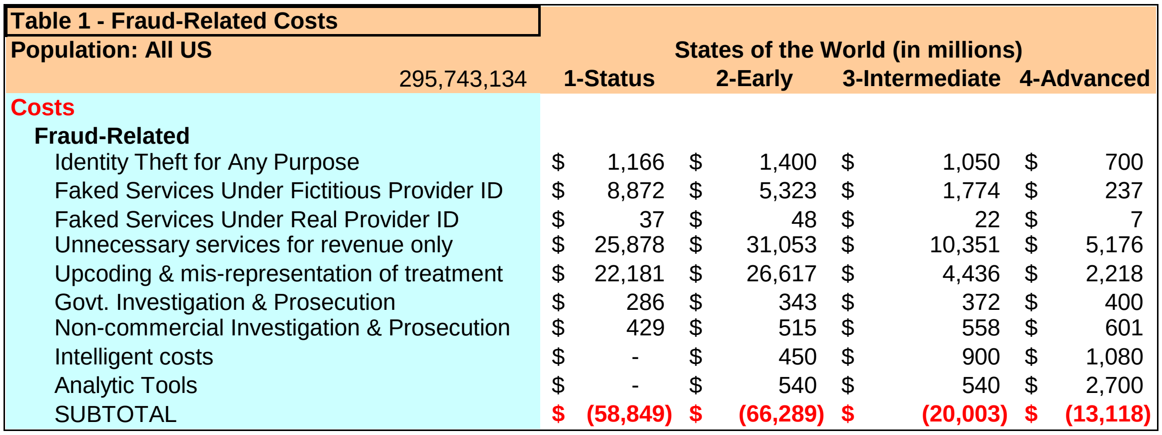


Table 1 - Fraud-Related Costs				
Population: All US	**States of the World (in millions)**			
295,743,134	**1-Status**	**2-Early**	**3-Intermediate**	**4-Advanced**
Costs				
Fraud-Related				
Identity Theft for Any Purpose	$ 1,166	$ 1,400	$ 1,050	$ 700
Faked Services Under Fictitious Provider ID	$ 8,872	$ 5,323	$ 1,774	$ 237
Faked Services Under Real Provider ID	$ 37	$ 48	$ 22	$ 7
Unnecessary services for revenue only	$ 25,878	$ 31,053	$ 10,351	$ 5,176
Upcoding & mis-representation of treatment	$ 22,181	$ 26,617	$ 4,436	$ 2,218
Govt. Investigation & Prosecution	$ 286	$ 343	$ 372	$ 400
Non-commercial Investigation & Prosecution	$ 429	$ 515	$ 558	$ 601
Intelligent costs	$ -	$ 450	$ 900	$ 1,080
Analytic Tools	$ -	$ 540	$ 540	$ 2,700
SUBTOTAL	**$ (58,849)**	**$ (66,289)**	**$ (20,003)**	**$ (13,118)**

[73] Sparrow, M.K., *License to Steal: Why Fraud Plagues America's Health Care System,* Westview Press, Boulder, Colorado, 1996., p. 137 (Describing predictability as a weakness, "Fully automated payment systems are completely predictable. And predictability is welcomed in such processing systems as a product of consistency, procedural correctness, and data-processing accuracy. But in the business of fraud control, perfect predictability is a flaw. Perfect predictability makes the target static, transparent, and easy to attack.").

[74] *License To Steal: Why Fraud Plagues America's Health Care System,* Malcolm K. Sparrow, Westview Press, Boulder, 1996 p. 189 (Quoting a recent article in *American Medical News*, "The new intelligent computing systems cast their nets constantly, tirelessly, and more thoroughly than the human examiners and limited computer programs they are replacing. Promoters claim that some o the new systems are so "smart" they can even train themselves.")

Table 2 – Non Fraud-Related Annual Costs

Table 2 captures the costs associated with the initial capital investments and the ongoing operating costs that must be made by healthcare providers in order to implement IT systems that increase in their intelligence and analytic capabilities. Given the dynamic nature of fraud, new detection tools are always needed to ferret it out. Funding has also proven to be the main barrier to the adoption of EHRs.

In addition to large up-front investment, cost-savings are only realized in the medium to long term.[75] The issue is not whether to implement the use of IT to detect fraud, but rather how to equip fraud management teams with the best technological tools possible.[76] Note that capital investment costs are considerably higher than operating costs. This model assumes that with increasing interoperability will come greater standardization of data elements and modularization of the features of the provider's EHR application and will lead to lowered or neutral changes in operating expenditures. In addition, costs for providers learning new systems are reflected in interoperability transition costs.

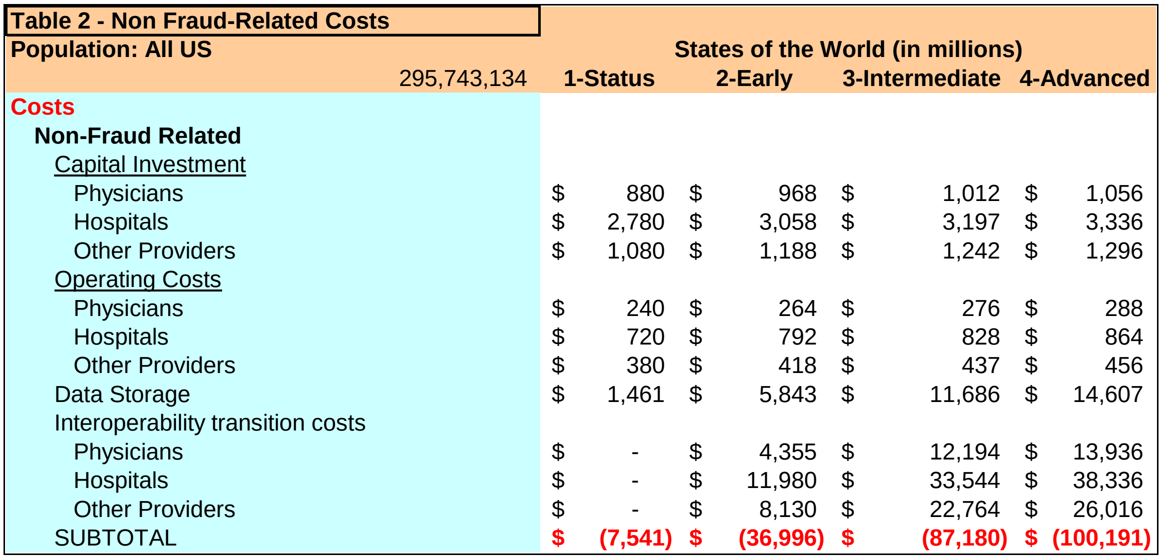


Table 2 - Non Fraud-Related Costs					
Population: All US		**States of the World (in millions)**			
	295,743,134	**1-Status**	**2-Early**	**3-Intermediate**	**4-Advanced**
Costs					
Non-Fraud Related					
Capital Investment					
Physicians		$ 880	$ 968	$ 1,012	$ 1,056
Hospitals		$ 2,780	$ 3,058	$ 3,197	$ 3,336
Other Providers		$ 1,080	$ 1,188	$ 1,242	$ 1,296
Operating Costs					
Physicians		$ 240	$ 264	$ 276	$ 288
Hospitals		$ 720	$ 792	$ 828	$ 864
Other Providers		$ 380	$ 418	$ 437	$ 456
Data Storage		$ 1,461	$ 5,843	$ 11,686	$ 14,607
Interoperability transition costs					
Physicians		$ -	$ 4,355	$ 12,194	$ 13,936
Hospitals		$ -	$ 11,980	$ 33,544	$ 38,336
Other Providers		$ -	$ 8,130	$ 22,764	$ 26,016
SUBTOTAL		**$ (7,541)**	**$ (36,996)**	**$ (87,180)**	**$ (100,191)**

[75] Brailer, D.J., Terasawa, E.L., *Use and Adoption of Computer-based Patient Records*, California HealthCare Foundation, October, 2003.

[76] Sparrow, M.K., *License to Steal: Why Fraud Plagues America's Health Care System,* Westview Press, Boulder, Colorado, 1996.

Table 3 – Fraud Management-Related Annual Benefits

Table 3 reflects the reality faced by the healthcare industry that emerging patterns of fraud seem to pass unnoticed until enormous amounts of damage are done.[77] Therefore, in the world of State 1, benefits are primarily derived from the recovery of funds only after the fraud has been committed. The benefits that are projected with the introduction of electronic health records coupled with e-prescribing in State 2 offer only a glimpse of the benefits that intelligent (State 3) and analytic (State 4) tools could offer in an interoperable environment.[78]

Table 3 - Fraud Management-Related Benefits					
Population: All US		**States of the World (in millions)**			
	295,743,134	**1-Status**	**2-Early**	**3-Intermediate**	**4-Advanced**
Benefits					
Fraud Management-Related					
Government Recovery		$ 1,144	$ 1,258	$ 2,860	$ 4,576
Private Sector Recovery		$ 458	$ 504	$ 687	$ 916
Conversion to ICD10		$ -	$ -	$ 90	$ 110
Digital tracing for Fraud		$ -	$ 53	$ 111	$ 111
Patient verification of Dx & Procedure		$ -	$ 89	$ 185	$ 185
Provider Verification of Dx		$ -	$ 1,800	$ 5,700	$ 8,400
Digital certificates & signatures		$ -	$ 786	$ 1,638	$ 1,638
Reduction in record retrieval time		$ -	$ 2,359	$ 5,504	$ 7,076
Authentication		$ -	$ 393	$ 819	$ 819
IDs only from card swipes		$ -	$ 393	$ 819	$ 819
Avoided time spent for fraudulent claims		$ 131	$ 786	$ 2,621	$ 3,931
SUBTOTAL		**$ 1,733**	**$ 8,422**	**$ 21,033**	**$ 28,581**

[77] License To Steal: Why Fraud Plagues America's Health Care System, Malcolm K. Sparrow, Westview Press, Boulder, p. 38, 1996.

[78] U.S. Department of Health and Human Services, *The Costs and Benefits of Moving to the ICD-10 Code Sets,* The RAND Corporation: The Science and Technology Institute, March 2004.

Table 4 – Non Fraud Management-Related Annual Benefits

Table 4 quantifies the substantial benefits that can be captured that are non-fraud related. In a State 4 interoperable world, the clinical and administrative benefits that would result from providers (hospitals and medical group practices) and independent laboratories, radiology centers, pharmacies, payers, and public health departments being able to exchange electronic data would be substantial.

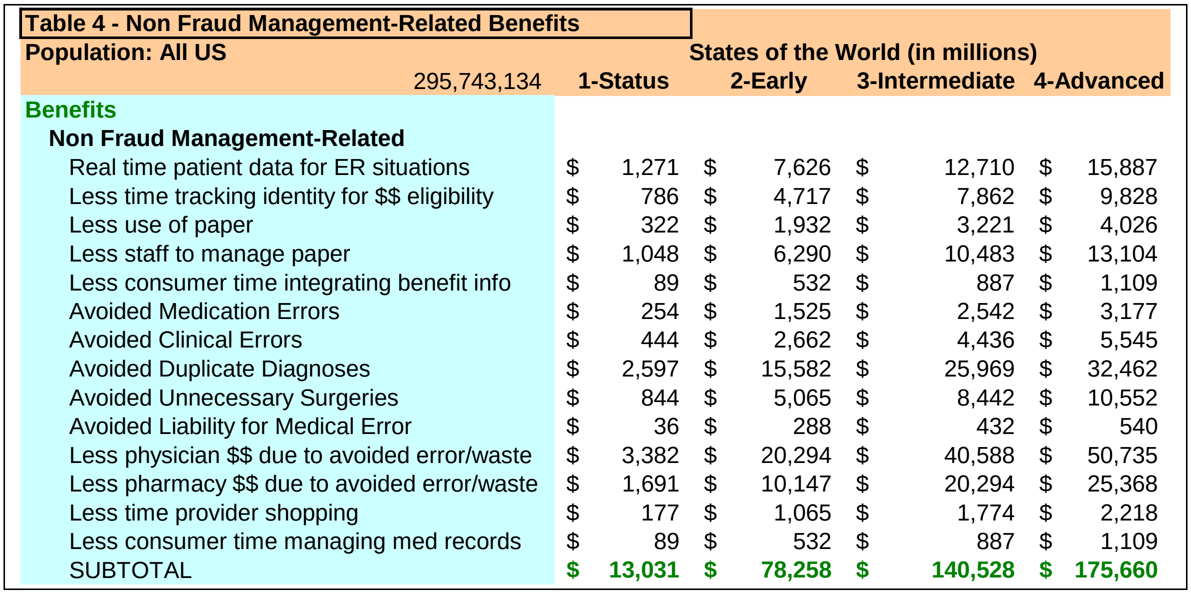


Table 4 - Non Fraud Management-Related Benefits					
Population: All US		States of the World (in millions)			
	295,743,134	1-Status	2-Early	3-Intermediate	4-Advanced
Benefits					
Non Fraud Management-Related					
Real time patient data for ER situations		$ 1,271	$ 7,626	$ 12,710	$ 15,887
Less time tracking identity for $$ eligibility		$ 786	$ 4,717	$ 7,862	$ 9,828
Less use of paper		$ 322	$ 1,932	$ 3,221	$ 4,026
Less staff to manage paper		$ 1,048	$ 6,290	$ 10,483	$ 13,104
Less consumer time integrating benefit info		$ 89	$ 532	$ 887	$ 1,109
Avoided Medication Errors		$ 254	$ 1,525	$ 2,542	$ 3,177
Avoided Clinical Errors		$ 444	$ 2,662	$ 4,436	$ 5,545
Avoided Duplicate Diagnoses		$ 2,597	$ 15,582	$ 25,969	$ 32,462
Avoided Unnecessary Surgeries		$ 844	$ 5,065	$ 8,442	$ 10,552
Avoided Liability for Medical Error		$ 36	$ 288	$ 432	$ 540
Less physician $$ due to avoided error/waste		$ 3,382	$ 20,294	$ 40,588	$ 50,735
Less pharmacy $$ due to avoided error/waste		$ 1,691	$ 10,147	$ 20,294	$ 25,368
Less time provider shopping		$ 177	$ 1,065	$ 1,774	$ 2,218
Less consumer time managing med records		$ 89	$ 532	$ 887	$ 1,109
SUBTOTAL		**$ 13,031**	**$ 78,258**	**$ 140,528**	**$ 175,660**

Table 5 – Summary of Annualized Cost and Benefits

Table 5 combines the estimated costs and benefits that were quantified in Tables 1 - 4, and provides the net values that can be expected based on the assumptions for each scenario. The modest increase in fraud related benefits of the early NHIN state is offset by the increase in fraud related costs, making this a wash from the fraud management standpoint.

It is not until States 3 and 4 that fraud management becomes truly net positive. This change occurs because interoperability has tremendous potential to lower fraud-related costs in States 3 and 4 because there will be more real time and near real time to corroborate the validity of online and automated transactions from multiple data sources for a given patient than in States 1 and 2.

Table 5 - Summary of Annualized Cost and Benefits					
Population: All US			**States of the World (in millions)**		
	295,743,134	**1-Status**	**2-Early**	**3-Intermediate**	**4-Advanced**
Costs					
Fraud-Related					
SUBTOTAL		**$ (58,849)**	**$ (66,289)**	**$ (20,003)**	**$ (13,118)**
Non-Fraud Related					
SUBTOTAL		**$ (7,541)**	**$ (36,996)**	**$ (87,180)**	**$ (100,191)**
Total		**$ (66,390)**	**$ (103,285)**	**$ (107,183)**	**$ (113,309)**
Benefits					
Fraud Management-Related					
SUBTOTAL		**$ 1,733**	**$ 8,422**	**$ 21,033**	**$ 28,581**
Non Fraud Management-Related					
SUBTOTAL		**$ 13,031**	**$ 78,258**	**$ 140,528**	**$ 175,660**
Total		**$ 14,764**	**$ 86,679**	**$ 161,561**	**$ 204,241**
Net Cost (-) Benefit (+) - Fraud Only		$ (57,116)	$ (57,867)	$ 1,030	$ 15,463
% Healthcare GDP		-3%	-3%	0%	1%
Net Cost (-) Benefit (+) - Fraud and Non-Fraud		$ (51,626)	$ (16,606)	$ 54,379	$ 90,932
% Healthcare GDP		-3%	-1%	3%	5%

Findings

There are three major findings from this analysis.

- Substantial savings in fraud-related expenditures may be possible from a move to an interoperable NHIN that are not realized in the Status Quo and early non-interoperable NHIN states.
- Moving to interoperability in State 3 may provide the most dramatic improvement in fraud net cost/benefit.
- The non-fraud related net benefits in States 3 and 4 are substantially higher than the fraud net benefits. Interoperability may more than pay for itself.

The early NHIN state is nearly as costly as the Status Quo state in terms of the net fraud-related costs and their impact on the US health economy. Some of the assumed extra costs in the Status Quo and Early NHIN states come from the new Medicare Part D fraud opportunities.[79] Similarly, in the spring of 2003, the Rand Corporation study of the costs and benefits associated with transitioning from the use of ICD-9 codes to ICD-10 codes indicated both positive and negative cost impacts. Among the benefits of the transition, it was estimated that use of the ICD-10 codes would generate between $100 million and $1 billion in fewer fraudulent claims being paid.[80]

However, it is important to note that any transition from Status Quo will bring with it a higher probability of fraud initially. Libicki and Brahmakulam suggested that a new coding system, such as ICD-10, would present an increased opportunity for fraud in the beginning, when people are less familiar with the new codes. It might be more difficult to detect potential duplicates, unbundled services, or up-coding of procedures during the transition when two versions of code sets would be in effect. In the longer term, it is possible that fraud could be reduced since ICD-10-CM and ICD-10-PCS are more specific and there are fewer "gray" areas in coding.[81]

[79] RX for Fraud: Scamsters Can't Wait for Medicare's New $720 Billion Pill Plan, Forbes, June 20, 2005. (stating that the ink was barely dry on the 2003 Medicare law, that in addition to Part D drug benefits also included a provision providing people over 65 with discount cards and other subsidies, when reports that fraudsters were targeting eligible seniors. As a precursor to the actual roll-out of Medicare Part D the magnitude of the losses due to fraud could be staggering.)

[80] Libicki, M., Brahmakulam, I., *The Costs and Benefits of Moving to the ICD-10 Code Sets,* p. xvi. The RAND Corporation Science and Technology Institute, March 2004. http://www.rand.org/pubs/technical_reports/2004/RAND_TR132.pdf site visited on 8/14/2005.

[81] Libicki, M., Brahmakulam, I., *The Costs and Benefits of Moving to the ICD-10 Code Sets,* p. xvi. The RAND Corporation Science and Technology Institute, March 2004. ("Most observers believe that ICD-10-CM and ICD-10-PCS are technically superior to their ICD-9-CM counterparts. If nothing else, they represent the state of knowledge of the 1990s rather than of the 1970s. They have also been deemed more logically organized, and they are unquestionably more detailed—by a factor of two in diagnoses (and twenty for injuries) and by a factor of fifty in procedures.")

Results from this analysis should be interpreted with caution. The estimates presented are based on an economic impact model populated by the result of empirical studies and expert estimates of the costs of fraud prevention and health IT transition costs. However, many elements required expert estimation. At the very least, this analysis provides a structure for new evidence to be added so that areas where only expert opinion is available can be replaced with new empirical findings.

It is important to recognize, also, that the aggregate economic analysis undertaken here does not consider the actual distribution of these benefits and costs among the individual stakeholders involved. Benefits and costs will not be distributed evenly among all stakeholders.

The finding that interoperability could pay for itself, without consideration of fraud and abuse prevention, is not new. Walker et al (2005) found a similar result. This analysis concurs with this finding using methods that are similar but not identical. In addition, the finding of a fraud-related net benefit further supports the value proposition of interoperability proposed by the NHIN.[82]

This analysis could be advanced by a continued exploration to detail the trajectory and timing of the different states of the world. Such an analysis would produce a more advanced set of findings that would describe 5-, 10-, and possible 15-year net benefit calculations. This type of analysis would be particularly helpful to ascertain the optimal length of time for the various states, specifically for the Early NHIN. Of course, a longer time horizon with a more complex digital infrastructure may not affect fraud prevention without continuing efforts and stewardship to thwart any new possible fraud schemes.

Two recommendations can be identified and merit further discussion and investigation from using the lens of an economic framework to look at the possibility of healthcare fraud management benefits from future states of the world that are associated with a reduction in a wasted share of the US health economy:

- **Attempt to reduce exposure to the Early NHIN state. Given that this state of the HIT world is associated with relatively high costs compared to its benefits, it seems prudent to limit this state as much as possible.** The Early NHIN state is somewhat of a misnomer in that it is not a temporary transition through which the entire NHIN moves on the way to interoperability. The NHIN will always be a heterogeneous federation of sub-networks that will, themselves, be evolving through various states. Therefore, pockets of non-interoperability will likely exist for the foreseeable future. It is important to recognize the additional costs and vulnerability of these non-interoperable components and to attempt to minimize them.

[82] Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W., Blackford, M., *The Value of Health Care Information Exchange and Interoperability,* Health Affairs Web Exclusive, January 2005.

- **Move to the NHIN with advanced analytic tools as quickly as possible.** Although interoperability, by itself, provides the most dramatic net cost/benefit improvement, the addition of advanced analytics provides a substantial improvement in both fraud and non-fraud related benefits.

These two recommendations from the economic model analysis have been incorporated into the overall Guiding Principles and Recommendations discussed below.

Summary and Recommendations

The ONC Anti-Fraud Project Executive Committee (the Executive Committee) was made up of 22 cross industry experts, including representatives of providers, payers, information technology, fraud investigative services, finance, and government. The Executive Committee convened in Washington, DC for two in-person meetings and convened three meetings via teleconference.

The Executive Committee members served on workgroups on each of the following topics: Guiding Principles; Economic Model; Fraud Management; Law Enforcement and Prosecution; and Information Technology and Infrastructure. The contributions of each workgroup resulted in Guiding Principles for each area of focus. These essential guidelines were then integrated and streamlined into the core Guiding Principles. The composition of the committee was designed to bring together an expert panel reflecting a diversity of roles and perspectives. Although broad consensus was achieved on the findings, principles and recommendations in this report, the committee did not attempt to reach unanimous agreement on every view expressed.

The Executive Committee offers the Guiding Principles and associated Recommendations presented in this report for AHIC's consideration and use as it begins the work of developing recommendations to HHS for achieving digital and interoperable health records within 10 years. The committee further recommends that additional work on healthcare fraud management be conducted and fully integrated with all other AHIC and ONC activities in FY 2006.

The report's Guiding Principles and Recommendations provide a suggested roadmap for AHIC to ensure that the NHIN's design will enable cost-saving anti-fraud activities and deter healthcare fraud. They call for comprehensive healthcare anti-fraud initiatives and fraud management programs.

Preamble

The following Guiding Principles and Recommendations were developed by the National Executive Committee, a multi-stakeholder group of experts with significant experience and insight about the US healthcare system, fraud management, health records, information management, and technologies. The principles are based on a solid understanding of the vulnerabilities of the system to individuals with the intent to defraud and of the opportunities that well-designed health IT offers. They are intended to guide policy makers and to support the needs of the vast majority of providers of services who are striving to comply with honesty to laws and requirements that affect billing and reimbursement. While many of the recommendations cannot currently be implemented, they identify the future technology, capability, and capacity that will be needed.

Guiding Principles and Recommendations

1. **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.**

   Recommendations:

   a. Develop enterprise management and operating policies for all stakeholders will render the NHIN inherently resistant to fraud and that support fraud management. Fraud management is defined as the prevention, detection, and prosecution of healthcare fraud.

   b. Build in as part of the NHIN infrastructure standards, procedures, and prototypes to facilitate nationwide healthcare fraud management.

   c. Certify electronic health record (EHR) software features and functions that are required or prohibited in the NHIN infrastructure to enable effective healthcare fraud management.

   Workgroup:

   The principle and recommendations originated from the Guiding Principles workgroup.

2. **EHRs and information available through the NHIN must fully comply with applicable federal and state laws and meet the requirements for reliability and admissibility of evidence.**

   Recommendations:

   a. Establish standards for the electronic maintenance, submission, and disclosure of health and financial information contained in the EHR. Standards should address completeness, accountability, access and availability, traceability, auditability (verifiability), identification, authentication, non-repudiation, integrity, digital certificate, digital signature, electronic signature, and public key infrastructure.

   b. Delineate data quality and electronic transmission standards.

   c. Adopt a national approach to making public key infrastructure and other data security technologies available to all constituents of the NHIN.

   d. Ensure that access to and disclosure of EHR content and other information available through the NHIN is consistent with health information privacy and security laws and other applicable laws.

Workgroup:

The principle and recommendations originated and are summarized from the Law Enforcement and Prosecution Workgroup.

Standards should address:

Completeness - In developing required, mandatory, or customary data fields of information in EHRs and billing records, the information must include complete information and be sufficient to fully satisfy support and communicate decisions made about services rendered and facilitate automated coding and billing purposes.

Accountability - Users of the EHR (In moving from a paper or hybrid environment to an interoperable HIT system) agree that the EHR/NHIN system must contain executed "terms and conditions agreements" as necessary among all the parties to the electronic process to ensure that all conditions of submission and receipt of data electronically are mutually known and understood, including potential criminal, civil, and administrative penalties for making fraudulent claims or false statements.

Access and availability - Access must be restricted (closed) to only approved, identifiable users for approved, identifiable purposes. Access to any backup databases must be appropriately maintained and restricted and made available at all times.

Traceability - This key critical principle relates to access and traceability. Access must be restricted (closed) to only approved, identifiable users. The system collects and preserves all transaction (and/or clinical or encounter) information, including:

- Content or substance of the transaction (for example, the text of a contract or claim).

- The processing of the transaction (such as when and from where a communication was sent and when and where it was received throughout all phases of the transaction recordation/submission process).

- Identities of all parties or individuals involved in creating, transmitting, and receiving the record or transaction and the identification of any changes those parties or individuals made to the record or transaction via the digital certificate and signature process referenced below.

Auditable (verifiable) - The system's electronic processes can be shown to gather, retain, and reproduce data that can be audited and verified to be accurate and to do so reliably and without alteration**.**

Identification - The EHR and/or interoperable HIT system includes processes to identify and verify the identities of authorized users who input, alter, and/or transmit information as well as the identify of each individual who is a party to an EHR entry or transaction.

Authentication - The system must authenticate the parties and the specific individuals involved in creating, modifying, or transmitting an EHR or transaction. Authentication is defined as a system that enables a recipient to positively verify the signer without direct communication with the signer and subsequently demonstrate to a third party, if needed, that the sender's identity was properly verified.

Biometric Authentication - Authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both unique to the individual and measurable. This includes authorization of electronic signatures. Furthermore, this applies to records stored offshore in addition to those maintained electronically in the United States.

Non-repudiation - The EHR and/or interoperable NHIT system must ensure that strong and substantial evidence is available to the recipient of the sender's identity, sufficient to prevent the sender from successfully denying having sent the data. This criterion includes the ability of a third party to verify the origin of the document.

Integrity - The EHR and/or interoperable HIT system must ensure that the recipient, or a third party, can determine whether the contents of the document (EHR and/or electronic transmission) have been altered during its transmission or altered or amended or sought to be amended by any party.

Storage and Security - EHRs and/or data transmitted and retained in an interoperable HIT system must be stored and be secure from access by unauthorized and unidentified persons or users. This applies to data stored in the United States and offshore. Records must be retained - unaltered, readable, and retrievable - and record retention must comply with all applicable laws and regulations. Records are to be readily available and in a readable format in the English language. Regardless of the physical location where the EHR is stored, the EHR must at all times be actually available, by legal process or as otherwise authorized by law, to patients, governmental and private payers, and law enforcement.

Record Retention - Record retention requirements must be a minimum of 10 years. Presumably, patients would want their EHRs to be preserved forever since they represent patient medical history, but this would not be true for transactional/billing records. Law enforcement would need, at a minimum, to replicate current retention requirements for transactional records (that is, 10 years for civil enforcement purposes).

Reliability - Unique EHRs and the interoperable HIT system must reliably and consistently do what they are supposed to do, perform as they are supposed to, use redundant or backup (of all transactions and changes) systems as necessary and therefore be reliable. If the IT system fails, there is a goal of always having access for law enforcement and all other purposes. Either redundant or backup information must be available if the system fails.

Digital Certificate - A digital certificate is a data record that, at a minimum: (1) identifies the certification authority issuing it; (2) names or otherwise identifies the certificate holder; (3) contains a public key that corresponds to a private key under the sole control of the certificate holder; (4) identifies the operational period; and (5) contains a serial number and is digitally signed by the Certification Authority issuing it.

Digital Signature - An EHR or transaction record in an interoperable HIT system must include a digital signature record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed. This relates to the transmittal, which creates a record/technology and authenticates that it was an unaltered transaction.

Electronic Signature - A method of signing an electronic message that identifies a particular person as the source of the message (or record) and identifies the person's approval of the information contained in the message. The importance of a focus on the electronic signature is its relevance to traceability to an individual or organization.

Public Key Infrastructure (PKI) - A structure under which a Certification Authority verifies the identity of applicants, issues, renews, and revokes digital certificates, maintains a registry of public keys, and maintains an up-to-date Certification Revocation List.

Private Key - The key of a key pair that is used to create a digital signature.

Public Key - The key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages (records or transactions) from the holder of the key pair.

Federal Executive agencies were required to provide for (1) "the option of the electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper;" and (2) "the use and acceptance of electronic signatures, when practicable." [83]

3. A standard minimum definition of a Legal Health Record (LHR) must be adopted for electronic health records (EHRs).

Recommendations:

a. Establish national standards for the EHR to be maintained as a business record and, as such, adopt maintenance, retention, and disclosure practices for it as a business record that meets the requirements for reliable and admissible evidence.

[83] Under the Government Paperwork Elimination Act (GPEA), Pub. L. No. 105-277, §§1701-1710 (1998) (codified as 44 U.S.C.A. § 3504 n. (West Supp. 1999)),

b. Establish national “EHR as the LHR” standards (using the current guidelines for paper health records as a generally accepted base) to address the transition from paper through hybrid to fully electronic health records.

Workgroup:

This principle originated in the Fraud Management Workgroup as a recommendation. Upon review, it is believed to be a Principle. All recommendations for this principle originated from the Law Enforcement and Prosecution Workgroup.

4. **Comprehensive Healthcare Fraud Management programs must enable rather than inhibit national EHR adoption.**

Recommendations:

a. Include fraud management features in the interoperable EHR without placing undue financial burden on the providers.

b. Design EHR fraud management features and functionality that will not disrupt the provider workflow or interfere with the patient care process.

c. Balance the development of fraud management programs on the NHIN with other priority interests and infrastructure design requirements, especially patient care.

Workgroup:

The principle and recommendations originated from the Guiding Principles workgroup.

5. **Healthcare Fraud Management is the responsibility of all healthcare stakeholders.**

Recommendations:

a. Disseminate definitions and guidelines to inform and address the impact and consequences of healthcare fraud on the economy; on patient health risk and on population health risk.

b. Inform stakeholders of the interpretation of healthcare fraud guidelines with regard to EHR documentation and coding.

c. Identify (consistent with current legal requirements) when and who has the right to access relevant portions of patient records (EHRs) through the standard mechanisms of the NHIN for the purpose of conducting fraud related audits.

Workgroup:

The principle originated from the Guiding Principles workgroup.

Recommendation 5a and 5b originated from the Fraud Management workgroup and 5c originated from the Guiding Principles workgroup.

6. **Increased consumer awareness of healthcare fraud and the role health information technology and EHRs play in its reduction can improve the effectiveness of healthcare fraud management programs.**

   Recommendations:

   a. Develop and deploy a consumer awareness program on the role of information technology in healthcare fraud and its ability to detect and assist consumers to personally minimize fraud.

   b. Emphasize the benefits of the NHIN and EHRs in the national fight against healthcare fraud in program content and publications.

   Workgroup:

   The principle and recommendations originated from the Information Technology Infrastructure and Implementation workgroup.

7. **EHR standards must define requirements to promote fraud management and minimize opportunities for fraud and abuse, consistent with the use of EHR's for patient care purposes.**

   Recommendations:

   a. Mandate the minimum infrastructure necessary to ensure that EHR systems are maintained to facilitate ongoing fraud management programs and fraud prosecution activities.

   b. Define the EHR system requirements to support accurate documentation of the clinical care process, minimizing the potential to facilitate fraudulent practices.

   c. Develop NHIN IT infrastructure requirements to match or link the electronic documentation of a patient's clinical events and other relevant data files with the corresponding claims to enable healthcare fraud management.

   d. Develop minimum NHIN IT infrastructure procedures and requirements for data management, data efficiency, data exchange, data availability, security, backup, disaster recovery, record alteration, record authentication, and record retention that can be audited and verified.

   Workgroup:

   The principle originated from the Fraud Management Workgroup.

   Recommendations 7a and 7b originated from the Fraud Management Workgroup.

   Recommendation 7c originated from the Information Technology Infrastructure and Implementation workgroup.

   Recommendation 7d originated from and is summarized from both the Law Enforcement and Prosecution Workgroup and the Information Technology Infrastructure and Implementation Workgroup.

8. **Standardized reference terminology and up to date classification systems that facilitate the automation of clinical coding are essential to the adoption of interoperable EHRs and the associated IT enabled healthcare fraud management programs.**

   Recommendations:

   a. Adopt uniform rules, regulations, and guidelines for standardized reference terminology and up to date classification systems across the country.

   b. Ensure that the organizations authorized to develop, deploy, and maintain such standards and guidelines assume ongoing responsibility to:

      - Provide clarity with a specific standard or guideline as required.

      - Publish and disseminate the standards or guidelines in a manner that is generally understood.

      - Respond in a timely manner to all requests for clarification of standards or guidelines.

   c. Inform the individuals and entities choosing to participate in medical commerce that they are responsible for knowing and understanding the standards and guidelines with respect to clinical coding and classification.

   Workgroup:

   The principle and recommendations originated from the Guiding Principles workgroup.

9. **Fully integrate and implement fraud management programs and advanced analytics software in interoperable EHRs and the NHIN to achieve all of the estimated potential economic benefits.**

   Recommendations:

   a. Begin by building national work plans with specific timeframes for the varying levels of the NHIN's interoperability and its integration with and implementation of advanced analytics software for aggregate data analysis.

   b. Minimize the period of automated transactions without interoperability across providers.

   c. Move to a NHIN with analytic tools applied to aggregate data as quickly as possible once interoperability is achieved.

   Workgroup:

   The principle and recommendations originated from the Economic Impact Workgroup and the Information Technology Infrastructure and Implementation Workgroup.

10. **Data required from the NHIN for monitoring fraud and abuse must be derived from its operations and not require additional data transactions.**

    Recommendations:

    a. Provide access to aggregate de-identified data generated in the normal operations of the NHIN, provided that the aggregation of data does not impose an obligation on the provider to generate data it would not otherwise have created for patient care.

    b. Assess the potential applicability of creating a Healthcare Information Sharing and Analysis Center (HISAC) as a component of a national fraud management program.

    Workgroup:

    The principle originated from the Guiding Principles workgroup.

    Recommendation 10a originated from the Fraud Management workgroup.

    Recommendation 10b originated from the Information Technology Infrastructure and Implementation workgroup.

Conclusions

Healthcare fraud is a major weakness in the United States' healthcare system and it affects its ability to provide quality care and enhance patient safety at an affordable cost. Escalating premium costs and the associated implications contribute to the need for deliberate deployment of the NHIN with interoperable EHRs.

The need for portable health information has never been more evident than it is in the aftermath of the devastation to the Gulf coast by Hurricane Katrina in September 2005. Many of the paper based health records of patients in the affected areas were either destroyed or inaccessible. A NHIN designed with fraud management requirements and interoperable EHRs would provide assurance against additional national financial losses due to fraud schemes following a national terrorist event or natural disaster.

Healthcare fraud hurts all stakeholders. The full extent of healthcare fraud is unknown as there are no systematic measurements for fraud statistics, monitoring, or reporting. Fraud is dynamic and evolving and, as such, requires ongoing active surveillance using information technology and aggressive consumer involvement. Vigorous prosecution of healthcare fraud is a powerful deterrent to fraud perpetrators

It is essential that fraud management programs be built into the NHIN infrastructure as part of its early design. Designing fraud management functionality into the NHIN has the potential to significantly reduce healthcare fraud losses. The interoperability between multiple EHRs is a major enabler of these loss reductions. Maximum benefit will be achieved by linking a claim with its corresponding documentation from an EHR, having the ability to access information in other EHRs regarding the same patient, and applying advanced analytics to aggregate clinical and financial databases. Without a deliberate effort to build fraud management into the NHIN, healthcare payers and consumers will be exposed to new and potentially increased vulnerability to electronically-enabled healthcare fraud.

The conventional thinking is that the adoption of EHRs and participation in an interoperable NHIN will be voluntary and not mandated. While there are certainly many understandable reasons for such an assumption, it is also apparent that those who are the most aggressive perpetrators of fraud will almost certainly opt out of the NHIN in order to avoid its anti-fraud capabilities. Thus, the architects of the NHIN and those involved with payment systems may want to consider the advantages and disadvantages of a system that at some point in the future might predicate payment of claims on participation in the NHIN, assuming of course that this becomes feasible technologically and economically. While such linkage would certainly increase the anti-fraud potential of the NHIN, strong consideration must be given to the fact that this might seem unduly coercive and could mandate significant added costs for certain providers.

National metrics for fraud management are required to systematically gauge and reduce healthcare fraud. Public and private stakeholder collaboration, as well as interstate cooperation, is also required to fight healthcare fraud. Such an anti-fraud enabled NHIN has the potential to identify emerging fraud schemes prior to payment. A shift from the current "pay and chase" fraud management programs to the proactive prevention of fraudulent claims prior to payment is made possible by interoperable EHRs and advanced analytics.

In conclusion, substantial savings in fraud-related expenditures would be enabled by a NHIN. It is important, however, to move quickly through the early transition state of the NHIN and achieve widespread adoption in order to maximize net savings.

Bibliography

Print

AHIMA, July 14, 2005. *Update to Practice Brief: Definition of the Health Record for Legal Purposes, Draft V6*.

AHIMA, Dougherty, Michelle. "Standard Terminology Helps Advance EHR." *Journal of AHIMA* 74, no.10 (November 2003): 59-60.

AHIMA Workgroup on Electronic Health Records Management. October 2004. *The Strategic Importance of Electronic Health Records Management. Appendix A: Issues in Electronic Health Records Management*. Journal of AHIMA 75, no.9, Web extra

AHIMA, 2001, Practice Brief: Definition of the Health Record for Legal Purposes.

AHIMA, June 1998, Practice Brief: Data Quality Management Model, Journal of AHIMA.

Amatayakul, M. June 2004. *Electronic Health Records: A Practical Guide for Professionals and Organizations.* American Health Information Management Association (AHIMA). ISBN: 1584261331

Amatayakul, M. December 2004. *Electronic Health Records: Strategies for Implementation.* Opus Communications. ISBN: 1578395178

Amatayakul, M., and Lazarus, S.S. April 2005. *Electronic Health Records: Transforming Your Medical Practice.* Medical Group Management Association (MGMA). ISBN: 1568292325
American Health Lawyers Association, Quest for Interoperable Electronic Health Records: A Guide To Legal Issues in Establishing Health Information Networks, EDITED BY KRISTEN ROSATI, ESQUIRE, AND MARILYN LAMAR, ESQUIRE, July 2005

American Association for Health Plans.2002. *The Factors Fueling Rising Healthcare Cost*. Washington, DC.

Armstrong, D. May 2, 2005. *MRI and CT Centers Offer Doctors Way to Profit on Scans Physicians Pay a Flat Fee For Procedures, Then Bill Insurers -- at Higher Rate*. Navigating Legal Landscape. The Wall Street Journal, Page A1.

Ash, J., Gorman P., et al. 2001. *Investigating physician order entry in the field: Lessons learned from a multicenter study*. Med info, 10 (part 2), Pages 1107-1111.

Atkinson, P., and Miller, D. July 2003. *Medical Office Practice.* Thomson Delmar Learning. ISBN: 1401813984

Baird, Zoë. June 1, 2005. *Building Trusted Information-Sharing Environments for National Security and Health Care*. Key Note Speech. Web-Enabled Government: Transforming the Business of Government. The e-Gov Institute.

Barrows R.C., Jr. and Clayton P.D. 1996. *Privacy, confidentiality, and electronic medical records*. J Am Med Inform Assoc, 3 (2):139-48.

Bazzoli, F., Senior Editor, Daily News. June 27, 2005. *Consultant predicts 30 percent growth rate for physician EMRs*. Healthcare IT News

Brailer, D. 2004. *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care*. Framework for Strategic Action. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology. Washington, DC.

Brailer, D., and Thompson T. 2004. *Health IT Strategic Framework*. Department of Health and Human Services. Washington, DC.

Brailer, D. 2004. *Translating Ideals for HIT into Practice*. Health Affairs, 4:318

Brailer, D., and Terasawa, E. 2003. *Use and Adoption of Computer-based Patient Records*. California Health Care Foundation. Oakland CA.

Brailer, D. June 30, 2005. Statement on Activities of the Office of the National Coordinator for Health Information Technology before The Committee on Commerce, Science, and Transportation Subcommittee on Technology, Innovation, and Competitiveness, United States Senate**.**

Broder, C. *Healthcare industry makes legislative push for IT.* Healthcare IT News.

Business Wire. October 6, 2004. *Towers Perrin Projects at 8% Increase in Employer-Sponsored Health Care Costs for 2005*.

Carter, J. March 2001. *Electronic Medical Records: A Guide for Clinicians and Administrators.* American College of Physicians (ACP). ISBN: 1930513011

Carter J., and Gray P. 1999. *Healthcare information technology: An overview*. University of Texas.

CMS CERT Program, 05-11929; Federal Register / Vol. 70, No. 116 / Friday, June 17, 2005 / Notices.

Personal Communication with Office of the National Coordinator for Health Information Technology. March 2, 2005. (Ref 22 in The Lewin Group Report).

Center for Medicare & Medicaid, Office of the Actuary, National Health Statistics Group. 2000. *An Overview of the U.S. Healthcare System: Two Decades of Change, 1980-2000*. Baltimore, MD.

Chin T. August 2004. *Hospitals are laying the groundwork for EMRs*. American Medical News.

Coile, R.C. October 2000. *The Paperless Hospital: Healthcare in a Digital Age.* Health Administration Press. ISBN: 1567931626

Connecting for Health. 2004. *Financial, Legal and Organizational Approaches to Achieving Electronic Connectivity in Healthcare*. New York, NY.

Connecting for Health, Markle Foundation. September 2004. *Connectivity in Healthcare: A Preliminary Roadmap from the Nation's Public and Private-Sector Healthcare Leaders*.

Daigrepont, J.P. November 2003. *Automating the Medical Record Second Edition.* American Medical Association (AMA). ISBN: 1579475450

Darby & Karni. 1973. *Free Competition and the Optimal Amount of Fraud*. Journal of Law & Economics, 16 (1): 67-88.

Data Nation. August 11, 2002. *US healthcare ICT spending opportunities*.

Davis, N., Lemery, C., et al. April 2005. *Identity Theft and Fraud—The Impact on HIM Operations*. AHIMA Practice Brief, Journal of AHIMA 76, No. 4, 64A-D.

deBrantes, F., Glaser, J, PhD, et al. 2005. *Financial Incentives for Adoption of Health Information Technology by Healthcare Deliverers*. eHealth Initiative Foundation, Business Briefing, US Healthcare Strategies, Pages 56-58.

DeLotto, R., Rozwell, C, et al. April 2005. *Use Gartner's COMPARE Cycle to Guide Anti-Money-Laundering Effort*. ID Number: G00127061.

Department of Veterans Affairs. 2004. *VA Current and Future Computerized Patient Record System*. Washington, DC.

Dunn, J., Fulper, C., et al. September 30, 2004. *Using Software to Detect Fraud, Waste and Abuse in Healthcare; A Working Paper*. 10000.138.161.161 WRP01;
Earley, A, Research Note, Commentary, Predicts 2005: Insurance Anti-Fraud Tools Will Gain Traction, November 2004

Early, Annemarie and Galimi, Joanne, Gartner: Deploy Detection Technologies to Cut Insurance Fraud and Abuse Publication Date: 20 April 2005 ID Number: G00127061

Economist. May 8, 2003. *Is IT a cure*?

Finucane, M. 2004. *Facing Down Health Care Cost: Winning Strategies for Automotive Industry*. Ernst & Young Health Sciences Advisory.

Galimi, J., and Earley, A. May 1, 2004. *Deploy Detection Technologies to Cut Insurance Fraud and Abuse*. With insurance fraud making headlines throughout the U.S., insurers must abandon manual techniques and adopt these automated fraud-detection technologies.

GAO Report, Health Information Technology. May 2005. *HHS Taking Steps to Develop National Strategy*. GAO-05-618.

Garsten, Ed. 2004. *GM health care bill tops $60 million: Cost adds $1,400 per vehicle, hurts competitiveness*. The Detroit News.

Gingrich, N. (Reviewer) with Pavey, D., and Woodbury, A. May 2003. *Saving Lives & Saving Money.* Alexis de Tocqueville Institution. ISBN: 0970548540

Glaser, J.P. (Reviewer). January 2002. *The Strategic Application of Information Technology in Health Care Organizations, Second Edition.* Jossey-Bass. ISBN: 0787959871

Goldsmith, J, September 2003. *Digital Medicine: Implications for Healthcare Leaders*. Health Administration Press. ISBN: 1567932118

Harrington, H.J., Esseling, K.C, et al. April 1997. *Business Process Improvement Workbook: Documentation, Analysis, Design, and Management of Business Process Improvement*. McGraw-Hill. ISBN: 0070267790

Hartley, C.P., and Jones, E.D. III. February 2005. *EHR Implementation: A Step-by-Step Guide for the Medical Practice*. American Medical Association (AMA). ISBN: 1579476430

Institute of Medicine. March 2001. *Crossing the quality chasm*. National Academy Press. Washington, DC.

Institute of Medicine. November 1999. *To Err Is Human: Building a Safer Health System*. Washington, DC.

Keagy, B. (Ed), and Thomas, M. (Ed). August 2004. *Essentials of Physician Practice Management.* Jossey-Bass. ISBN: 0787971898

Kocieniewski, D., and Sullivan, J. July 6, 2005. *Medical School Double-Billed U.S. for Years*.

Kohn L.T., Corrigan J.M., et al (Editors). 2000. *To err is human: Building a safer health system*. National Academy Press. Washington, DC.

Kotter, J.P., and Cohen, D.S. June 2002. *The Heart of Change: Real-Life Stories of How People Change Their Organizations*. Harvard Business School Press. ISBN: 1578512549

Lang R.D. Winter 2001. *An Incremental Approach to a Web-Based Computerized Medical Record*. Journal of Healthcare Information Management. 15 (3).

LaTour, Kathleen and Eichenwald, Shirley, Health Information Management Concepts, Principles and Practice, AHIMA, 2002

Lovitky, Jeffrey and Ahern, Jack, *Designing compliance programs that foster ethical behavior,* Healthcare Financial Management, March, 1999

McKenna, M., and Sands, D. (Ed). March 2003. *High Tech Medicine: Building Your Medical Practice with Computers and the Internet.* Fordham University Press. ISBN: 1886761299

Middleton. July 2004. *A paperless healthcare system?* Business Week.

Miller R. and Sim I. 2004. *Physician's Use of Electronic Medical Records: Barriers and Solutions*. Health Affairs, 23:2.

Murphy, G., Waters, K., et al. March 1999. *Electronic Health Records: Changing the Vision.* W.B. Saunders Company. ISBN: 0721673864

National Healthcare Anti-Fraud Association. April 2005. *Health Care Fraud A Serious and Costly Reality For All Americans*. Washington, DC.

Office of the Press Secretary. Executive Order 13335. April 27, 2004. *Incentives for the Use of Health Information Technology and Establishing the Position of National Health Information Technology Coordinator*. Washington, DC.

Parente, S, PhD, Kim, S., PharmD, et al. *Drug Safety Identifying Controlled Substance Patterns of Utilization Requiring Evaluation Using Administrative Claims Data*. The American Journal of Managed Care, Vol. 10, No. 11, Pages 783-790.

Pear, Robert. June 28, 2005. U.S. Report Faults States' Medicaid Tactics; The New York Times. Washington DC.

Signs of Fraud Go Beyond Signature**,** Credit Card Companies Use Artificial Intelligence to Thwart Thieves, By Margaret Webb Pressler, Washington Post Staff Writer
Sunday, July 21, 2002; Page H05

Sparrow, M. December 1998. *Fraud Control in the Health Care Industry: Assessing the State of the Art*. National Institute of Justice Research in Brief, Pages 1 – 11.

Sprague L. 2004. *Electronic health records: How close? How far to go?* (800):1-17. NHPF Issue Brief.

Tang, P. July 31, 2003. *Key Capabilities of an Electronic Health Record System: Letter Report*. Institute of Medicine. Washington, DC.

The Lewin Group. March 2005. Health Information Technology Leadership Panel Final Report.

United States Government Accountability Office (GAO), Report to the Chairman, Committee on the Budget, House of Representatives. May 2005. *Health Information Technology/HHS Is Taking Steps to Develop a National Strategy*.

Vardi, Nathan. June 20, 2005. *Prescription for Fraud*. Forbes Magazine.

Wacther R. 2005. *The End of the Beginning: Patients Safety Five Years After 'To Err is Human'*. Health Affairs, 30.

Wager, K., Glaser, J.P., et al. May 2005. *Managing Health Care Information Systems: A Practical Approach for Health Care Executives*. Wiley, John & Sons. ISBN: 0787974684

Walker, J.M., Bieber, E.J., and Richards, F. February 2005. *Implementing An Electronic Health Record System*. Springer. ISBN: 1852338261

Walker, J., Pan, E., et al. 2004. *The Value of Health care Information Exchange and Interoperability*. Center for Information Technology Leadership. Boston MA.

Wang, S., Middleton, B., et al. April 2003. *A cost-benefit analysis of electronic medical records in primary care*. American Journal of Medicine, 1; 114(5): pages 397-403.

Watson, J. June 29, 2005. *Anti-fraud team saves NHS £675m; Unit analyses millions of transactions to detect fraud*. Computing. ttp://www.computing.co.uk/computing/news/2139071/anti-fraud-team-saves-nhs-675m

Economist Looks at Barriers to Health IT. May 5, 2005. Investor's Business Daily Interviews Brailer on Health IT Issues.

Gartner's COMPARE Cycle provides a useful and well-understood framework for monitoring ongoing compliance efforts. The five-step Cycle defines activity levels, provides a standard for measuring compliance progress and delineates milestones toward neutralizing the threat of compliance failures. Publication Date: 26 April 2005. ID Number: G00127063.

Parallel Pathways for Quality Healthcare: A Framework for Aligning Incentives with Quality and Health Information Technology. May 25, 2005. Recommendations of the Working Group for Financing and Incentives eHealth Initiative and Foundation.

The Legal Aspects of the Electronic Health Record. May 10, 2005. Unpublished work product of the HL7 Work Group on legal aspects of the EHR.

Web

FORE Body of Knowledge at www.ahima.org
AHIMA e-HIM^{TM} Work Group on Health Information Management in a Hybrid Environment. *The Complete Medical Record in a Hybrid EHR Environment, Parts I-III*.

http://www.hhs.gov/healthit/frameworkchapters.html ONC Homepage and Health IT Strategic Framework

http://niri.ncsa.uiuc.edu/martirano/medex/medIT.html
An Overview of Medical Informatics.

http://www.homecaremag.com/mag/medical_target/
Are You a Target? April 1, 2004.

www.AFPonline.org
Association for Financial Professionals. March 2005. *Payments Fraud and Control Survey Report of Survey Results.*

http://www.hipaafaq.com/cpri.htm
Blair, Jeffrey S., Program Manager, IBM Healthcare Solutions.
An Overview of Healthcare Information Standards. Atlanta, GA.

http://releases.usnewswire.com/redir.asp?ReleaseID=44207&Link=http://www.usnewswire.com/
Blue Cross and Blue Shield Plans File $30 Million Lawsuit Alleging Rent-A-Patient Fraud in Southern California; Scheme has Bilked Tens of Millions of Dollars from Consumers and Insurers. 3/11/2005.

www.onlinepressroom.net/bcbsa
Blue Cross and Blue Shield System's Antifraud Efforts Save $157 Million.

http://www.cms.hhs.gov/manuals/107_som/som107ap_a_hospitals.pdf
CMS Condition of Participation for Hospitals #482.24.

http://www.sgc.gc.ca/publications/policing/Identity_Theft_Consumers_e.asp *Public Advisory: Special Report for Consumers on Identity Theft*.

http://www.cybersource.com/developers/*ecommerce developer, tools kit, e commerce, e-commerce, commerce*.

http://sev.prnewswire.com/computer-electronics/20041101/SFM00701112004-1.html
EverBank Chooses Quova for Fraud Prevention-Online Banking Giant Selects GeoPoint for Identity Verification.

http://tmlr.net/jump/?c=14346&a=296&m=3197&p=1617018&t=164 Consumers Recognize Value of EMRs Says Accenture Study, July 27, 2005, Neil Versel

http://www.consumer.gov/idtheft
Federal Trade Commission. *Your National Resource for ID Theft*.

http://www.afsimage.com/Solutions/CheckProcessing/FraudDetection
Fraud prevention, detection and signature verification – AFS Signature verification, fraud prevention and fraud detection for check processing.

http://www.healthcareitnews.com/NewsArticleView.aspx?ContentID=2907
Frist, B. (R-Tenn, Senate Majority Leader). *On healthcare IT requirements*.

http://www.stopidentitytheft.org/
Georgia Stop Identity Theft Network.

http://www.healthdatamanagement.com/HDMSearchResultsDetails.cfm?DID=19130
Goedert, Joseph. *Industry Responds to Call for I.T*. Network Ideas.

http://www.healthmgttech.com/archives/bus0499.html
Hellerstain, MD, PhD. *The Business of Healthcare/HIPAA's Impact on Healthcare/In the Spotlight-Fraud and Abuse Provisions. Are Security and Privacy Implications Lurking in the Shadows of HIPAA?*

http://www.mgforex.com/eng/about/content/laundering.asp
About MG Financial GroupMoney laundering occurs when funds from an illegal/criminal activity are moved through the financial system in such a way as to make it appear that the funds have come from legitimate sources

http://oig.hhs.gov/fraud.html
HHS-OIG-Fraud Prevention & Detection.

http://oig.hhs.gov/fraud/advisoryopinions.html
HHS-OIG-Fraud Prevention & Detection - Advisory Opinions Fraud Prevention & Detection Advisory Opinions. Advisory Opinions Frequently Asked.

http://www.himss.org/content/files/ehrattributes070703.pdf
HIMSS Electronic Health Record Definitional Model, Version 1.1. September 24, 2003.

http://www.stopfraud.bcbsmt.com/Identify/id_fraud.html
How to identify Health Care Fraud.

http://www.identitytheft.org/
Identity Theft Prevention and Survival.

http://www.privacyrights.org/identity.htm
Identity Theft Resources.

http://www.idtheftcenter.org/ Identity Theft Resource Center | A Nonprofit Organization -

http://www.insideid.com/idtheft/
Inside ID Identity Theft Prevention Consumers rely on credit card transactions to make secure purchases online. Identity theft threatens to disrupt consumer confidence in ecommerce and the Internet. Learn how to use identity management -

http://www.quova.com/solutions/internet-fraud-detection.shtml
Internet Fraud Detection, Online Fraud Prevention with Geolocation.

http://www.healthleaders.com/magazine/cover.php
Justice Joins Caremark Whistleblower Suit. Cover story July 2005.

http://identitytheft.articleinsider.com/171817_bank_account_fraud.html
Larsen, C. *Bank Account Fraud and Awareness by Customers*.

http://www.maxmind.com/app/ccv_overview
MaxMind - Overview of Credit Card Fraud Detection (CCFD) Services*.*

http://www.medicare.gov/FraudAbuse/Tips.asp
Medicare Fraud Prevention and Detection Tips.

http://www.ncua.gov/Publications/brochures/identityTheft/
National Credit Union Administration. *You Can Fight Identity Theft*.

http://www.nasact.org/washconnection/downloads/2005/062405.pdf
NECCC ID Theft/Fraud Workgroup Invites Participants to Join Work on Major Project.

http://www.nytimes.com/2005/06/28/politics/28medicaid.html?ex=1120622400&en=df150b9fa73fa60d&ei=5070&emc=eta1
Pear, Robert. June 28, 2005. *U.S. Report Faults States' Medicaid Tactics*.

http://www.priestongroup.com/battling.asp
Prieston, A., and Dreyer, J. 1999. *Battling Fraud With Tougher Documents*. Originally published in *Mortgage Banking*.

http://www.sas.com/industry/banking/fraud/index.html
SAS Fraud Detection and Prevention.

http://accounting.smartpros.com/x33375.xml
SmartPros Accounting.

www.hhs.gov/ocr/hipaa
Standards for Privacy of Individually Identifiable Health Information; Final Rule. 45 CFR Part 164.501. Federal Register 65, No. 250 (August 14, 2003).

http://www.aaai.org/Pathfinder/html/fraud.html
The Guardian. September 9, 2004. *Fraud Detection & Prevention/Mimicking fraudsters*.

http://www.darmouth.edu/~cecs/index.html
Trustees of Dartmouth College. From Center for the Evaluative Clinical Sciences (CECS) at Dartmouth.

http://www.hipaadvisory.com/news/NewsArchives/2005/0223pandab.htm
US Divided on Privacy Risks of Electronic Medical Records. February 23, 2005. Hackensack, NJ

http://www.efunds.com/
Visa USA Adds Another Layer of Technology to Help Member Financial Institutions Prevent Fraud; Card Application Screening Expanded through an Association with eFunds.

https://host.softworks.ca/agate/ama_posp/public/abouttxt.asp Physician Office System Program Homepage,

http://www.healthleaders.com/magazine/cover.php?contentid=69883 Health Leaders, Jul. 2005, Cover story, Sharing the Data Bridge

http://waysandmeans.house.gov/hearings.asp?formmode=view&id=2944 Statement of David Brailer, M.D., Ph.D., National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. Testimony Before the Subcommittee on Health of the House Committee on Ways and Means, July 27, 2005.

http://www.wedi.org/cmsUploads/pdfUpload/Generic/pub/2005-01EHRwhitepaper.pdf, Background on EHR for Small Practices/White Paper, January 2005

http://www.whitehouse.gov/news/releases/2005/01/20050127-2.html The White House, President George W. Bush, Improving Care and Saving Lives Through Health IT

https://www.oxhp.com/main/fraud/affects.html United Healthcare, Oxford Benefit Management.

http://www.nhcaa.org/pdf/all_about_hcf.pdf National Health Care Anti Fraud Association, 2005

http://www.ckfraud.org/ckfraud.html National Check Fraud Center Homepage

http://www.cms.hhs.gov/glossary Centers for Medicare and Medicaid Services, Glossary

http://www.managedhealthcareexecutive.com/mhe/article/articleDetail.jsp?id=173378, Advanced analytics are a powerful secret weapon against healthcare fraud, August 1, 2005, Andrea Allmon, MD, Managed Healthcare Executive

http://www.managedhealthcareexecutive.com/mhe/article/articleDetail.jsp?id=173378 Advanced analytics are a powerful secret weapon against healthcare fraud, August 1, 2005, Andrea Allmon, MD, Managed Healthcare Executive

http://www.managedhealthcareexecutive.com/mhe/article/articleDetail.jsp?id=96834 Fraud and abuse applications pique payers' interests, Joanne Galimi, Managed Health care ExecutiveMay 2004

http://www.questia.com/PM.qst?a=o&d=5002005009, Health Care Fraud, Journal article by Jonathon Cone, Marisa Levinson, Shelley Finlayson, American Criminal Law Review, Vol. 40, 2003

http://www.nap.edu/books/0309090776/html/ Patient Safety: Achieving a New Standard for Care, National Academies Press (2004)

http://www.healthcare-informatics.com/issues/2004/11_04/trends.htm, Healthcare Informatics, News & Trends - Healthcare Informatics HEALTH INFRASTRUCTURE/Industry takes step toward EHRs, November 2004

www.ahima.org Body of Knowledge

www.whatis.com

www.aishealth.com/EhealthBusiness/EhealthTerms.html

http://www.advancedhealth.com/glossary

http://legal-dictionary.thefreedictionary.com

http://www.hhs.gov/healthit/glossary

http://www.cms.hhs.gov/glossary/

http://www.fairisaac.com/Fairisaac/Solutions/Enterprise+Decision+Management/Business+rule Fair Isaac Corporation 2005

Acknowledgements

This report was prepared by FORE for the Office of the National Coordinator for Health Information Technology (ONC). FORE gratefully acknowledges those who participated in the interview process and/or facilitated site visits for this project. The information captured as a result of these interviews and site visits was crucial to the development of the findings in this report. The organizations represented included private sector businesses and government organizations. FORE gratefully acknowledges the cooperation and assistance of the Executive Committee members, including the leadership provided by David Brailer, MD, PhD, Coordinator for Health Information Technology, DHHS and Kathleen Fyffe, MHA, Project Officer.

Appendix A - Interview Questions

1. What types of fraud do you think will be enabled by use of electronic health records (EHRs) or a widespread health information infrastructure? Can you anticipate new threats? If so, please specify.

2. What technologies can be deployed to prevent, detect, and prosecute healthcare fraud activities in the following two scenarios:

    a. EHRs without a nationwide network

    b. Interoperable EHRs with a nationwide network

3. What management practices should be considered to prevent, detect, and prosecute healthcare fraud activities in the following two scenarios:

    a. EHRs without a nationwide network

    b. Interoperable EHRs with a nationwide network

4. How can the consumer assist in preventing, detecting, and prosecuting healthcare fraud activities in the following two scenarios:

    a. EHRs without a nationwide network

    b. Interoperable EHRs with a nationwide network

5. What advances/practices can be borrowed from the credit card and banking industry to prevent, detect, and prosecute fraud in the following two scenarios:

    a. EHRs without a nationwide network

    b. Interoperable EHRs with a nationwide network

6. Consider how information flows from clinical encounter to payment. What are the weak links in the movement of information (such as provider, patient, payer, and employer) and what opportunities do they create for fraud?

7. As interoperable EHRs are being deployed:

    a. What guiding principles do you recommend to recognize the role of law enforcement as business users of health information to prevent, detect, and prosecute healthcare fraud?

    b. What guiding principles do you recommend for infrastructure development and implementation to maximize fraud prevention, detection, and prosecution?

    c. What specifically can be done to counter anticipated new threats?

8. What must be done to preserve evidence and manage records to facilitate fraud prosecution in the following two scenarios:

    a. EHRs without a nationwide network

    b. Interoperable EHRs with a nationwide network

9. What do you view as the weak links in anti-fraud software, education, and compliance practices today? Will a fully functioning network of interoperable EHRs assist in strengthening or eliminating these links? If so, how?

10. What laws or regulations need to be enacted or changed to facilitate fraud prevention, detection and prosecution in the following two scenarios:

    a. EHRs without a nationwide network

    b. Interoperable EHRs with a nationwide network

11. Does your agency have any specific requirements or concerns that haven’t been identified or discussed in a previous question?

Appendix B – Executive Committee

Co-Chairs

Arnold Milstein, MD, MPH

Dr. Milstein is the Medical Director of the Pacific Business Group on Health (PBGH) and Chief Physician at Mercer Human Resource Consulting. PBGH is the largest healthcare purchasers' coalition in the U.S. Dr. Milstein's work and publications focus on healthcare purchasing strategy, clinical performance measurement, and the psychology of clinical performance improvement. He co-founded both the Leapfrog Group and the Consumer-Purchaser Disclosure Project. He heads performance measurement activities for both initiatives and is a MedPAC Commissioner. Previously a Rosenthal Lecturer at the Institute of Medicine, the New England Journal of Medicine's series on employer-sponsored health insurance described him as a "pioneer" in efforts to advance quality of care. In 2004 and 2005, he received the highest annual award of World-at-Work, the largest global organization of human resource managers, and of the National Business Group on Health. Educated at Harvard (BA Economics), Tufts (MD), and UC Berkeley (MPH Health Services Evaluation and Planning), he is an associate clinical professor at the University of California at San Francisco.

Donald W. Simborg, MD

Dr. Simborg is an independent consultant. He was co-founder of HL7, the healthcare data interchange organization and a founding member of the American College of Medical Informatics. Author and/or editor of over 100 articles, chapters, and books on a wide range of medical informatics topics, he was Founder and CEO of iKnowMed, a company providing an electronic medical record for medical oncology practices, sold to US Oncology in July 2004. Dr. Simborg was founder and CEO of Simborg Systems Corporation, a network-based patient care system for hospitals, sold to Bell Atlantic Corporation in 1990. He remained as CEO of Bell Atlantic Healthcare Systems for three years. He formerly served as a member of the Computer Science and Telecommunications Board of the National Research Council, National Academy of Sciences. Dr. Simborg received his medical degree from Johns Hopkins and is board certified in Internal Medicine. He is a former Associate Professor of Medicine at Johns Hopkins and the University of California, San Francisco.

Members

A. John Blair, III, MD

John Blair, III, MD is the president and CEO of the Taconic IPA, a 2,300 physician independent practice association in New York's Mid-Hudson Valley. Dr. Blair founded MedAllies, a technology enabling company focused on physician office support and systems interoperability that leverages the Internet to integrate the healthcare community. Dr. Blair has been instrumental in advancing a regional pay-for-performance program focusing on technology, adoption, and usage. Dr. Blair is a Board-Certified General Surgeon with fifteen years in private practice. Dr. Blair received his medical degree from Rush Medical School in Chicago and did his surgical training at the University of Texas Medical Center in Dallas. He performed a Gastrointestinal fellowship at the Middlesex Hospital in London, England.

Robert B. Burleigh, CHBME

Mr. Burleigh is President of Brandywine Healthcare Services, an international consulting practice specializing in financial management and compliance for medical practices, medical billing companies, practice management systems, and regulatory compliance. Bob is a member, lecturer, and/or author for organizations including the Healthcare Billing and Management Association, HCCA, AFEHCT, HFMA, AHLA, MGMA, AHA, AAHAM, American College of Emergency Physicians, Radiology Business Management Association, American Collectors Association, and many others. He is a Director and Past President of HBMA and an Advanced Member of HFMA. He is a Certified Healthcare Billing and Management Executive (CHBME) and a graduate of Penn State University (B.S. Business Management).

Rebecca S. Busch, RN, MBA, CCM, CBM, CHS-III, CFE, FHFMA

Ms. Busch is President and Chief Executive Officer of Medical Business Associates. She is a registered nurse and holds an MBA. She is also a certified fraud examiner (CFE), health care fellow in financial management (FHFMA) and internal auditor (formal CIA accreditation pending). In 1991, Rebecca founded Medical Business Associates, with the vision of delivering a multi-disciplined approach to conducting comprehensive audits for Major Employers, Hospitals, and Insurance Companies. Ms. Busch currently has a patent pending in the area of medical and financial errors in healthcare; has testified as an expert in the area of health care reimbursement, life care expense analysis, patient care documentation and respective damages; and she is currently writing a "how to" book that will teach American families how to detect fraud in reviewing their own families' medical bills.

Timothy J. Coleman, JD

Tim Coleman is Senior Counsel to the Deputy Attorney General at the U.S. Department of Justice. He advises the Deputy Attorney General on white-collar crime and serves as Special Counsel for Health Care Fraud, coordinating the work of Department of Justice components handling healthcare fraud matters. He also works closely with the President's Corporate Fraud Task Force. Previously, Tim served as Counsel to Assistant Attorney General Christopher Wray in the Criminal Division of the Department of Justice. Tim served for six years as an Assistant U.S. Attorney in the Southern District of New York, and was a member of that office's Securities and Commodities Fraud Task Force. He won the Chief Postal Inspector's Award for his work on corporate fraud matters. He is a graduate of Georgetown Law School and was previously in private practice at Cravath, Swaine & Moore in New York.

Kenneth F. Faustine

Mr. Faustine is currently Fraud Manager in the Special Investigations Unit responsible for the investigation of Healthcare Insurance Fraud nationwide. Prior to entering the private insurance industry, he was with the Internal Revenue Service, Criminal Investigation Division for 28 years. He has published articles in the Financial Crimes Report and the Journal of the National Association of Attorneys General and has acted as a reviewer for training textbooks published by the Health Insurance Association of America. Mr. Faustine holds a Masters Degree in Accounting, is a Certified Fraud Examiner and a member of the National Health Care Anti-Fraud Association.

Donna Hoffmeier

Ms. Hoffmeier is Vice President, Government Affairs - Strategy and Policy for UnitedHealth Group. Previously, she was the Vice President of Public Policy and External Affairs for Ovations; principal of Astra Solutions, LLC, a government relations consulting firm that specialized in healthcare policy and federal procurement; senior Washington representative for Highmark Blue Cross/Blue Shield; and worked in the federal government for over fifteen years. She graduated from the University of South Florida cum laude with a B.A. in Mass Communications and is pursuing a graduate degree in Public Relations at the University of Maryland.

Byron Hollis, Esq., CFE, AHFI

Byron Hollis is the Managing Director of the BlueCross BlueShield Association’s National Anti Fraud Department. In this capacity, he is responsible for providing national strategic leadership and support to the anti fraud programs at 40 independent BlueCross and BlueShield companies, who collectively insure over 93 million customers. In addition, Mr. Hollis is responsible for direction and leadership of BCBSA, FEP-Special Investigations Unit. Mr. Hollis is a graduate of Auburn University and the Thomas Goode Jones School of Law. He is a licensed attorney (State of Alabama). Mr. Hollis joined the staff of BlueCross BlueShield of Tennessee in 1995 and was the Investigations Coordinator for the BCBST, Special Investigations Unit, until 2002, when he was appointed to lead the BlueCross BlueShield Association’s National Anti-Fraud Director’s Office.

Richard Ingraham

Mr. Ingraham is Sr. National Industry Strategist for SAS US Commercial - Health & Life Sciences, Strategy, Alliance & Solutions. Rick has served in various executive capacities across both commercial and governmental entities within the healthcare and insurance industries. Since joining SAS Institute in 1998, Richard's efforts have been directed toward working with customer senior level management teams in their efforts to improve strategic decision making processes and knowledge management. Charged with setting the vision for SAS's contribution specifically within the health payer sector, he has identified the key SAS focus areas for this sector as improvement of the disease management process; detection and prevention of fraudulent claims; provider performance reporting and profiling; consumer driven health plan analytics; and customer profitability intelligence.

Stephen L. Jones, DHA

Dr. Stephen Jones is the Principal Deputy Assistant Secretary of Defense for Health affairs following 30 years of administrative liaison experience in public, legislative, educational, and private settings, and as a consultant in government relations, business development, and strategic planning. Dr. Jones holds a Bachelor of Science degree from Clemson University, a Master of Social Work from the University of South Carolina, and a Doctorate of Health Administration from the Medical University of South Carolina. Dr. Jones is a member of the Board of Directors for the South Carolina Federal Credit Union, the South Carolina Biotechnology Incubation Program and the Scenic Black River Advisory Council. He served as a U.S. Army military intelligence officer from 1968 to 1970, with tours in Washington, D.C. and Turkey.

Holly Louie, CHBME, BSN

Holly Louie is a Certified Healthcare Billing and Management Association (HBMA) Executive and a Registered Nurse, BSN and is currently an independent healthcare consultant with Practice Management, Inc. An active member of HBMA, she currently serves on their Board of Directors, and is a past Chair of the National Coding Committee, National Ethics and Compliance Committee, and co-developer of the HBMA Compliance Implementation Course for Billing Companies. She also assisted in draft revisions of OIG Guidance for Third Party Billers. Ms. Louie holds a BS in Nursing from the University of Alabama in Huntsville and is a member of HBMA, AHLA, and HCCA.

Jeff J. Matza, AHFI, CFE

Jeff Matza, AHFI, CFE, is the Vice President, Special Investigations, for Mutual of Omaha and he is responsible for directing the investigation of internal and external fraud, embezzlement, and questionable business practices. Mr. Matza has spoken to diverse audiences on the subject of insurance fraud, including topics such as Health Care Fraud Evidence and Collection, Dental Fraud, Internal Diversion of Assets, as well as numerous Special Investigative Unit (SIU) management issues. He has been a frequent presenter for the National Health Care Anti-Fraud Association, the Federal Bureau of Investigation, and was also a joint presenter with the Department of Justice in providing healthcare fraud training to members of New Scotland Yard in the United Kingdom. Matza is the former Chairperson of the Institute for Healthcare Fraud

Prevention and he is the current Vice-Chairperson of the National Healthcare Anti-Fraud Association.

Lewis Morris, Esq.

Lewis Morris is the Chief Counsel in the Office of Inspector General, Department of Health and Human Services. He works with a staff of over 60 attorneys and other professionals to provide a wide range of services to the OIG, as well as guidance to the healthcare industry. He is responsible for coordinating OIG′s role in the investigation and resolution of healthcare fraud cases, including cases brought under the civil False Claims Act. Prior to serving as the Chief Counsel to the Inspector General, Lew served in a variety of capacities within the OIG and the Office of General Counsel.

Maureen Mudron, JD

Maureen Mudron is Washington counsel at the American Hospital Association (AHA) and she is currently engaged in projects related to hospital billing and collections, tort reform, hospital–physician relationship issues, appropriate enforcement and implementation of EMTALA, clear guidance, and fair enforcement of Medicare payment requirements (that is, physician self-referral, the government's anti-fraud activities). Prior to joining the AHA, Maureen was with the Illinois Department of Mental Health and Developmental Disabilities and served as Chief Legal Counsel. Maureen is a graduate of The John Marshall Law School, Chicago IL, and received her undergraduate degree from the University of Illinois, Champaign. She is a member of the American Health Lawyers Association and the American Bar Association.

Alison Rein, MS

Alison Rein is the Assistant Director of Food and Health Policy at the National Consumers League (NCL). Ms. Rein is currently engaged in the development of several projects designed to enhance the safe use of medications, improve consumer access to product information, and highlight food safety and nutrition issues. Prior to joining NCL, Ms. Rein served as a healthcare consultant to a number of organizations for which she conducted strategic evaluations, marketing campaigns, and cost-effectiveness analyses of numerous drug, biologic, and device interventions. She has designed and conducted marketing research projects among manufacturers, healthcare payers, providers of care, and patients. Ms. Rein has co-authored several articles published in peer-review journals.

Beth Schermer, JD

Ms. Schermer is a partner at Coppersmith Gordon Schermer Owens & Nelson, P.L.C. with over 25 years of experience in the health law field. She represents healthcare systems, hospitals, and provider groups. As general counsel to the Arizona Hospital and Healthcare Association, Ms. Schermer has been actively involved in the development of healthcare legislation and initiatives in the areas of Medicaid/AHCCCS reimbursement, tobacco tax and tobacco settlement funds for healthcare purposes, quality review and confidentiality, advanced directives, and patient privacy. She served as President of the American Health Lawyers Association in 2000/2001 and on the Association's Board and Executive Committee from 1997 to 2002. In 2005, she was appointed to the inaugural class of Fellows of AHLA. She graduated from Harvard Law School in 1980.

James Speros, JD

Mr. Speros is the Manager of the Evaluation and Assessment Service of the Veterans Health Administration's national Office of Compliance and Business Integrity. Prior to joining VA, Mr. Speros served as General Counsel or equivalent to insurance holding companies in Ohio and Illinois, an Assistant Director of the Ohio Department of Insurance, as Trustee of a multi-hospital county healthcare system in Ohio, and as President of the Ohio Association of Managed Care Organizations. Mr. Speros is a Fellow of the Ethics Resource Center, a member of the Health Care Compliance Association, the Health Care Anti-Fraud Association and the Health Care Compliance Association. He holds a Bachelor of Science from Boston University and a J.D. from Cleveland-Marshall College of Law.

Jonathan Topodas, JD

Jonathan currently serves as Vice President and Counsel in Aetna's Federal Government Relations area responsible for federal health legislative and regulatory matters. Jonathan has been with Aetna since his graduation from Southern Methodist University School of Law in 1974. During this period, he has provided legal counsel to a number of Company clients as a member of the Law Department and more recently as a member of Federal Government Relations section of the Law Department. As head of Aetna's health office in Washington, Jonathan works with numerous employer groups including the U.S. Chamber, the National Association of Manufacturers, the National Business Group on Health and the American Benefits Council, where he is a Member of the Board of Directors.

Jean de Traversay

Mr. de Traversay is the Director of Healthcare Analytics at Fair Isaac Corporation. His extensive background in commercial health insurance and in clinical research has enabled him to contribute in both technical and business aspects to the Fair Isaac Corporation's Healthcare Group since its inception in 1997. He has participated in the development and implementation of many fraud detection models for Medicare, several Medicaid programs, several commercial carriers and pharmacy benefit managers, as well as for the Australian Medicare system. His earlier role as a senior statistician at PacifiCare Health Systems and the Southern California Permanente Medical Group concentrated on the development and fine-tuning of quality assessment projects and payment system initiatives.

Susan Turney, MD, MS, FACP, CMPE

Susan L. Turney, MD, MS, FACP, CMPE, is the Executive VP/ CEO of the Wisconsin Medical Society. She earned her medical degree and Master's degree in health administration from the University of Wisconsin, and completed her internal medicine residency at Marshfield Clinic/Saint Joseph's Hospital. Dr. Turney serves on the AMA Advisory Committee of Group Practice Physicians, is a fellow of the American College of Physicians, and serves as Vice Chair of the Medical Group Management Association Board of Directors. In her role as Chief Executive Officer of the Society, Dr. Turney is spearheading efforts that will lead to healthcare that is accessible, affordable, effective, timely, and safe for all of Wisconsin's patients.

Alan Yuspeh, JD, MBA

Alan Yuspeh is Senior Vice President, Ethics, Compliance and Corporate Responsibility for the Hospital Corporation of America (HCA). HCA owns and operates about 180 hospitals and related healthcare facilities. Prior to joining HCA , Mr. Yuspeh worked as Legislative and Administrative Assistant to United States Senator J. Bennett Johnston, Jr. of Louisiana; General Counsel to the United States Senate Armed Services Committee; a partner and associate in several large Washington law firms (during which time he coordinated the defense industry ethics initiative); and a consultant with McKinsey & Company. Mr. Yuspeh holds a BA degree from Yale, an MBA degree from Harvard, and a JD degree from Georgetown.

Executive Committee Liaisons

Marsha C. Massey, Esq.

Marsha Massey is the Affirmative Civil Enforcement (ACE) Coordinator and, at the time of the compilation of this report, the Acting Health Care Fraud Coordinator for the Executive Office for United States Attorneys in Washington DC. In her position, she coordinates the civil enforcement efforts of the 94 United States Attorneys Offices, serves as a legal advisor on ACE and healthcare fraud matters, and acts as a point of contact for and liaison to the United States Attorneys community for those matters. Previously, Marsha served as an Assistant U.S. Attorney in the Southern District of Indiana where she was the Civil Health Care Fraud Coordinator and co-chaired the district's Health Care Fraud Task Force. Marsha has been awarded the HHS Inspector General's Integrity Award for her work in health care fraud. She earned her law degree from Stetson University College of Law and received her undergraduate degree in economics from Wake Forest University.

Steve Shandy

Steve Shandy is a Senior Program Analyst in the U.S. Department of Justice, Criminal Division, Fraud Section, where he provides analytic and research support for the Department's health care fraud enforcement program. In this capacity, Mr. Shandy works closely with the Centers for Medicare and Medicaid Services on a variety of interagency health care fraud enforcement initiatives. Previously, Mr. Shandy worked in the Department's Office of Policy and Legislation where he assisted in designing and implementing the pilot program for President Clinton's 100,000 COPS grant program and the initial COPS awards. Mr. Shandy has a graduate degree in American Government from the University of Maryland-College Park and a bachelor's degree from Washburn University in Topeka, KS.

Appendix C – Project Staff

Susan P. Hanson, MBA, RHIA, FAHIMA

Ms. Hanson, the Project Director/Task 2, is the President of TerraStar Consulting Services. Previously, Susan was COO of Wang Healthcare Information Systems, COO and EVP for Medicus Systems Corporation, and Director of Patient Data Services at the University of Washington in Seattle, WA. While COO at Wang Healthcare, Ms. Hanson worked directly with physician practices of all sizes to successfully implement Wang's EHR/HIT solution. At Medicus, Ms. Hanson was responsible for the company's products and services including automated coding and grouping software. From 1995 through 1997, Susan served as a member of the National Research Council's Computer Science and Telecommunications Board's Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, which published *For the Record, Protecting Electronic Health Information, 3/5/97.* She is a Past President of American Health Information Management Association and the Washington State Health Information Management Association. She earned an Executive MBA from the University of Washington in Seattle and a BS in Medical Record Science from Daemen College.

Kathleen H. Fyffe, MHA

Ms. Fyffe, the Project Officer, is a senior advisor working in the newly established Office of the National Coordinator for Health Information Technology (ONC) at the U.S. Department of Health and Human Services (HHS). She has 20 years of experience working on information technology in hospitals, physician faculty practice plans, health maintenance organizations, and long-term care facilities. Before joining HHS in 2001, Kathleen was the Federal Regulatory Director at the Health Insurance Association of America, a national trade association. From 1997 to 2001 Ms. Fyffe held an appointed position on the National Committee on Vital and Health Statistics, which is an independent advisory committee to the Secretary Health and Human Services. Ms. Fyffe received a Master of Health Administration degree from Duke University and a Bachelor of Arts degree from Wake Forest University.

Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS

Ms. Cassidy, the Project's Senior Research Associate, is President of Cassidy & Associates which is dedicated to HIM consulting services. Bonnie's previous work experience includes consulting as a Vice President with Precyse Solutions, Principal with North Highland, Senior Manager at Ernst & Young and Price Waterhouse, and HIM Administrator for two major teaching hospitals in Cleveland. Bonnie is an active volunteer serving AHIMA as Chair of the Fellowship Review Committee, newly elected to the AHIMA Board of Directors and member of the CAHIIM Panel of Surveyors. She is a member of the Certification Commission for Health Information Technology (CCHIT) Certification Process Work Group. Her achievements include the Legacy Award and Professional Achievement Award from AHIMA and the Distinguished Member Award from the Ohio Health Information Management Association (OHIMA).

Stephen Parente, PhD, MPH, MS

Dr. Parente, the Project's Health Economist, is an Assistant Professor in the Department of Finance at the Carlson School of Management at the University of Minnesota where he specializes in health insurance, medical technology evaluation, health economics, and outcomes research. He holds an appointment as adjunct faculty member at Johns Hopkins University Bloomberg School of Public Health. Prior to joining the University of Minnesota faculty, Dr. Parente served as a Legislative Fellow in the office of Senator John D. Rockefeller IV (D-WV) during the health reform initiatives of the Bush and Clinton administrations. He has a doctorate from Johns Hopkins University and both a Masters of Science in public policy analysis and a Masters of Public Health from the University of Rochester.

Richard W. Singerman, PhD

Dr. Richard Singerman serves as an Expert in the US Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONCHIT) headed by Dr. David Brailer. With an expertise in healthcare strategic innovation and corporate knowledge sharing, Dr. Singerman leads multiple programs in health information technology adoption including measuring the national adoption rate of electronic health records (EHRs), assessing the economic impact of the EHR adoption gap, and framing a national vision around clinical decision support. Dr. Singerman was previously the Director of Innovation Advancement for Ascension Health and also served as a Principal with the Venture Consulting and Digital Strategy Group of Headstrong, Inc. He has also run his own firm offering product design services to healthcare and communication technology clients including *idealab!* and Stanford Telecom. Dr. Singerman has also been a National Research Council postdoctoral fellow at the National Institutes of Health, and served on the Planning & Value Committee and the Information Technology Working Group of the Health Technology Center and on the Board of Directors of the MIT Enterprise Forum of Washington/Baltimore.

Dr. Singerman has a BS in physics from the Massachusetts Institute of Technology, a BA and Advanced Certificate of Mathematics from Cambridge University, England, where he was a Marshall Scholar, and a PhD in physics from Cornell University.

FORE Representatives

Linda L. Kloss, MA, RHIA

Linda L. Kloss, MA, RHIA, has served as CEO of the American Health Information Management Association (AHIMA) since 1995. Kloss serves on the Board of Directors for AHIMA and FORE. In her role at AHIMA, Linda is responsible for delivering services to the fast changing HIM community, promoting its mission and values, and executing the Association's strategic plan. Kloss led the Association's efforts to co-found the Certification Commission for Healthcare Information Technology and she currently serves on the Steering Committee of Connecting for Health; the Board of Directors for the National Alliance for Health Information Technology; and the Leadership Council for the e-Health Initiative. Prior to joining AHIMA in 1995, Kloss served as one of the founding officers for MediQual Systems, Inc. and InterQual, Inc.

Eileen M. Murray, MM, CFRE, CAE

Ms. Murray has more than twenty years of experience in leading non-profit organizations in strategic planning and resource development. In her current position, she provides leadership and direction to the program, fundraising, and communications efforts of the Foundation. She holds an M.M. in Marketing with a concentration in Public and Non-Profit Management from the Kellogg Graduate School of Management at Northwestern University and has credentials as a Certified Fundraising Executive (CFRE) and Certified Association Executive (CAE).

Appendix D - Workgroup Participants

Guiding Principles

Leader

Donald W. Simborg

Members

A. John Blair III

Rebecca Busch

Arnie Milstein

Maureen Mudron

Alison Rein

James Speros

Fraud Management

Leader

Donald W. Simborg

Members

Robert Burleigh

Rebecca Busch

Donna Hoffmeier

Dan Leeper (FBI)

Beth Schermer

John Topodas

Michelle Dougherty (AHIMA staff)

Rita Scichilone (AHIMA staff)

IT Infrastructure and Implementation

Co-Leaders

Rebecca Busch

Jean de Traversay

Members

Richard Ingraham

Holly Louie

Economic Impact

Leader

Stephen Parente

Members

Rebecca Busch

Byron Hollis

Susan Turney

Alan Yuspeh

Law Enforcement and Prosecution

Co-Leaders

Jim Speros

Marsha Massey (DOJ)

Members

Rebecca Busch

Kenneth Faustine

Jeff Matza

Lewis Morris

Maureen Mudron

Steve Shandy (DOJ)

Appendix E - Definitions

Abuse

A range of the following improper behaviors or billing practices including, but not limited to billing for a non-covered service, misusing codes on the claim (that is, the way the service is coded on the claim does not comply with national or local coding guidelines or is not billed as rendered), or inappropriately allocating costs on a cost report.

Abuse Control

Limiting program access to only authorized persons. Methods include user IDs and passwords. Access control can be based on roles, status of a situation (for example, emergencies), physical location, or functions. Policies and procedures for access control are an integral part of the HIPAA regulation. Access control does not necessarily mean authentication of users. It is an important step for any organization involved in e-health today. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation.

Access and availability

Access must be restricted (closed) to only approved, identifiable users for approved, identifiable purposes. Access to any backup databases must be appropriately maintained and restricted, and made available at all times.

Access to Information

The ability or the means necessary to read, write, modify, or communicate data and/or information or otherwise make use of any system resource.

Adjudication

Processing claims according to contract.

Aggregate Data

Data extracted from individual patient records and combined to form information about groups of patients.

Antitrust

A legal term encompassing a variety of efforts on the part of government to assure that sellers do not conspire to restrain trade or fix prices for their goods or services in the market.

Architecture

A term that is often applied to overall system design, structure, and components of software and hardware, its operating system, or a network.

Auditable (verifiable)

The system's electronic processes can be shown to gather, retain, and reproduce data that can be audited and verified to be accurate, and to do so reliably and without alteration**.**

Audit trail

A software tracking system to trace the history of who used the computer, when they used it, and what information was accessed as well as a history of any actions taken by them to computer files or programs. Audit trail is mandated by HIPAA regulation for patients' medical information.

Authentication

Methods to confirm the user's identity, preliminarily by user ID and password, but it may require other technologies such as biometrics (electronic capture and analysis of patterns of finger printing, retinal scans or voice recognition) or Public Key Infrastructure (PKI). Proof of authorship.

Authorization

Any document designating any permission. The HIPAA Privacy Rule requires authorization or waiver of authorization for the use or disclosure of identifiable health information for research (among other activities). The authorization must indicate whether the health information used or disclosed is existing information/or new information that will be created. The authorization form may be combined with the informed consent form, so that a patient need sign only one form. An authorization must include the following specific elements: a description of what information will be used and disclosed and for what purposes; a description of any information that will not be disclosed, if applicable; a list of who will disclose the information and to whom it will be disclosed; an expiration date for the disclosure; a statement that the authorization can be revoked; a statement that disclosed information may be redisclosed and no longer protected; a statement that if the individual does not provide an authorization, the individual may not be able to receive the intended treatment; the subject's signature and date.

Authorization management

The process of protecting the security and privacy of data in a database.

Beneficiary

A person designated by an insuring organization as eligible to receive insurance benefits.

Business Rules

Business rules can be anything an organization uses to make an operational decision. They might include enterprise, divisional, corporate, and line of business policies, as well as calculations and formulas, risk thresholds, and regulatory authorizations.

Rules are often expressed—in conversation, written text, and software—as “If, then” statements: “If the loan applicant does not have a sufficient credit history, then pull a report from a debit bureau.”

Clearinghouse

A service providing connectivity between healthcare providers (physicians, hospitals, and so forth) to payers (HMOs, insurers, government entities such as Medicare). Clearinghouses take claims, eligibility requests, claim status checks, and so forth from providers in various formats and then translate and reformat them according to the specifications by payers and re-transmit them to their original destination. As a value-added service they may add edit functions to check the validity and completeness of the claims. HIPAA allows providers to use clearinghouses without using standard transaction code sets specified in HIPAA regulations.

Clinical Data

Data captured during the process of diagnosis and treatment.

Clinical Data Repository

The component of an electronic health record that accepts, files, and stores clinical data over time from a variety of supplemental treatment and intervention systems for purposes such as practice guidelines, outcomes management, and clinical research. May also be called a data warehouse.

Clinical Decision Support

The capability of a data system to provide key data to physicians and other clinicians in response to "flags" or triggers that are functions of embedded, provider-created rules. A system that alerts case managers that a client's eligibility for a certain service is about to be exhausted is one example of this type of capability. Clinical decision support is also a key functional requirement to support clinical or critical pathways.

Coded Data

Data are separated from personal identifiers through use of a code. As long as a link exists, data is considered indirectly identifiable and not anonymous or anonymized. Coded data is not covered by the HIPAA Privacy Rule, but is protected under the Common Rule.

Coding

The process of assigning alphabetic and/or numeric representations to clinical information.

Completeness

In developing required, mandatory, or custom data fields of information in EHRs and billing records, the information must include complete information and be sufficient to fully satisfy support and communicate decisions made about services rendered and facilitate automated coding and billing purposes.

Compliance

Accurately following the government's rules on Medicare billing system requirements and other federal or state regulations. A compliance program is a self-monitoring system of checks and balances to ensure that an organization consistently complies with applicable laws relating to its business activities.

Confidentiality

The protection of individually identifiable information as required by state or federal law or by policy of the healthcare provider. A legal and ethical concept that establishes the healthcare provider’s responsibility for protecting health records and other personal and private information from unauthorized use or disclosure.

Data Backup Plan

A documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information.

Data Condition

A description of the circumstances in which certain data are required.

De-identified

Under the HIPAA Privacy Rule, data are de-identified if either (1) an experienced expert determines that the risk that certain information could be used to identify an individual is "very small" and documents and justifies the determination, or (2) the data does not include any of the following eighteen identifiers (of the individual or the individual’s relatives, household members, or employers) that could be used alone or in combination with other information to identify the subject: names, geographic subdivisions smaller than a state (including zip code), all elements of dates except year (unless the subject is greater than 89 years old), telephone numbers, FAX numbers, e-mail address, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers; certificate/license numbers; vehicle identifiers including license plates, device identifiers and serial numbers; URLs; Internet protocol addresses; biometric identifiers; full face photo and comparable images; and any unique identifying number, characteristic or code. Even if these identifiers are removed, the Privacy Rule states that information will be considered identifiable if the covered entity knows that the identity of the person may still be determined.

Digital Certificate

Digital certificate is a data record that, at a minimum: (1) identifies the certification authority issuing it; (2) names or otherwise identifies the certificate holder; (3) contains a public key that corresponds to a private key under the sole control of the certificate holder; (4) identifies the operational period; and (5) contains a serial number and is digitally signed by the Certification Authority issuing it.

Digital Signature

An EHR and/or transaction record in an interoperable HIT system must include a digital signature record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer’s identity and the integrity of the file can be confirmed. This relates to the transmittal, which creates a record/technology and authenticates that it was an unaltered transaction.

Disclosure

The release of identifiable health information regarding a patient or patient(s). Disclosure involves the release of information to anyone or any entity outside the covered entity.

Designated Record Set

A healthcare provider's medical and billing records about individuals and any records used by the provider to make decisions about individuals. Individuals, including research subjects, have the right under the HIPAA Privacy Rule to access and amend protected health information in a Designated Record Set.

Electronic Health Record (EHR)

A real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision-making. The EHR can automate and streamline a clinician's workflow, ensuring that all clinical information is communicated. It can also prevent delays in response that result in gaps in care. The EHR can also support the collection of data for uses other than clinical care, such as billing, quality management, outcome reporting, and public health disease surveillance and reporting.

A term for the process of replacing the traditional hospital and physician practice paper-based medical records and integrating this information with patient financial data through automated electronic means; generally includes the collection of patient-specific information from various supplemental treatment systems, such as a day program and a personal care provider; its display in graphical format; and its storage for individual and aggregate purposes.

This technology, when fully developed, meets provider needs for real-time data access and evaluation in medical care. Together with clinical workstations and clinical data repository technologies, the EHR provides the mechanism for longitudinal data storage and access. A motivation for healthcare entities to implement this technology derives from the need for medical outcome studies, more efficient care, speedier communication among providers, and management of health plans. One goal of HIPAA is to protect identifiable health information as the system moves from a paper-based to an electronic health information system.

Electronic Medical Record (EMR)

A term for the process of replacing the traditional paper-based chart through automated electronic means; generally includes the collection of patient-specific information from various supplemental treatment systems, for instance a day program and a personal care provider; its display in graphical format; and its storage for individual and aggregate purposes. Also called “digital medical record” or “electronic medical record.”

Electronic Signature

A method of signing an electronic message that identifies a particular person as the source of the message (or record) and identifies the person’s approval of the information contained in the message. The importance of a focus on the electronic signature is its relevance to traceability to an individual or organization.

Encryption

Software coding procedure to prevent hacking or illegal accessing by persons not intended. Encryption converts plain text into a disguised file or message using a mathematical algorithm. Security is enhanced with encryption that increases the complexity of time and processing power to decrypt files and messages. Currently, 128-bit encryption is the highest commercially available encryption algorithm.

Evidence

Every type of proof legally presented at trial (allowed by the judge) that is intended to convince the judge and/or jury of alleged facts material to the case. It can include oral testimony of witnesses, including experts on technical matters, documents, public records, objects, photographs, and depositions (testimony under oath taken before trial). It also includes so-called "circumstantial evidence" that is intended to create belief by showing surrounding circumstances that logically lead to a conclusion of fact. Comments and arguments by the attorneys, statements by the judge, and answers to questions that the judge has ruled objectionable are not evidence. Charts, maps and models that are used to demonstrate or explain matters are not evidence themselves, but testimony based upon such items and marks on such material may be evidence. Evidence must survive objections of opposing attorneys that it is irrelevant, immaterial, violates rules against "hearsay" (statements by a party not in court), and/or other technicalities.

Explanation of Benefits (EOB)

The statement the beneficiary receives after you file a claim with your insurance company or a claim has been filed on your behalf by the doctor. This statement is a summary of the action taken on your claim—how much of the bill was paid by the third party payer/insurance company and how much is your responsibility to pay (you may already have paid that portion at the time of service).

Federal Health Architecture (FHA)

A collaborative body composed of several federal departments and agencies, including the Department of Health and Human Services (HHS), the Department of Homeland Security (DHS), the Department of Veterans Affairs (VA), the Environmental Protection Agency (EPA), the United States Department of Agriculture (USDA), the Department of Defense (DoD), and the Department of Energy (DOE). FHA provides a framework for linking health business processes to technology solutions and standards and for demonstrating how these solutions achieve improved health performance outcomes.

Fraud

Intentional misrepresentations that can result in criminal prosecution, civil liability, and administrative sanctions.

Fraud and Abuse Legislation

Federal laws that address the intentional and mistaken misrepresentation of reimbursement claims submitted to government sponsored health programs.

Guideline

A policy or rule intended to give practical guidance

Healthcare Fraud

Criminal health care fraud: “knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program or 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.” (Title 18, United States Code § 1347)

Civil health care fraud: any person who—

(1) knowingly presents, or causes to be presented, to an officer or employee of the United States Government or a member of the Armed Forces of the United States a false or fraudulent claim for payment or approval;

(2) knowingly makes, uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the Government;

(3) conspires to defraud the Government by getting a false or fraudulent claim allowed or paid;

(4) has possession, custody, or control of property or money used, or to be used, by the Government and, intending to defraud the Government or willfully to conceal the property, delivers, or causes to be delivered, less property than the amount for which the person receives a certificate or receipt;

(5) authorized to make or deliver a document certifying receipt of property used, or to be used, by the Government and, intending to defraud the Government, makes or

delivers the receipt without completely knowing that the information on the receipt is true;

(6) knowingly buys, or receives as a pledge of an obligation or debt, public property from an officer or employee of the Government, or a member of the Armed Forces, who lawfully may not sell or pledge the property; or

(7) knowingly makes, uses, or causes to be made or used, a false record or statement to conceal, avoid, or decrease 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…" [84] (Title 31 U.S.C. §§ 3729-3733)

Health Information

Information in any form (oral, written, or otherwise) that relates to the past, present, or future physical or mental health of an individual. That information could be created or received by a healthcare provider, a health plan, a public health authority, an employer, a life insurer, a school, a university, or a healthcare clearinghouse. All health information is protected by state and federal confidentiality laws and by HIPAA privacy rules

Health Information Technology (HIT)

The application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of healthcare information, data, and knowledge for communication and decision making.

Health Level Seven (HL7)

A data interchange protocol for healthcare computer applications that simplifies the ability of different vendor-supplied information systems to interconnect. Although not a software program in itself, HL7 requires that each healthcare software vendor program HL7 interfaces for its products.

Hearsay

A statement other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.

[88] For purposes of the False Claims Act, the terms "knowing" and "knowingly" mean that a person, with respect to information--
(1) has actual knowledge of the information;
(2) acts in deliberate ignorance of the truth or falsity of the information; or
(3) acts in reckless disregard of the truth or falsity of the information,
and no proof of specific intent to defraud is required.

Identification

The EHR and/or interoperable HIT system includes processes to identify and verify the identities of authorized users who input, alter, and/or transmit information and the identities of each individual who is a party to a EHR entry or transaction

Integrity

The EHR and/or interoperable HIT system must ensure that the recipient, or a third party, can determine whether the contents of the document (EHR and/or electronic transmission) have been altered during its transmission or altered or amended or sought to be amended by any party.

Interoperability

The applications used on either side of a communication, between trading partners and/or between internal components of an entity, being able to read and correctly interpret the information communicated from one to the other

Law Enforcement Official

An officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to: (1) Investigate or conduct an official inquiry into a potential violation of law; or (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Medical Informatics

The systematic study, or science, of the identification, collection, storage, communication, retrieval, and analysis of data about medical care services (data and information used to diagnose, treat, cure and prevent disease) to improve decisions made by physicians and managers of healthcare organizations. Medical informatics is as important to physicians and medical managers as the rules of financial accounting are to auditors.

National Payor ID

A system for uniquely identifying all organizations that pay for healthcare services. Also known as Health Plan ID or Plan ID.

National Provider ID

A system for uniquely identifying all providers of healthcare services, supplies, and equipment.

Nonrepudiation

The EHR and/or interoperable NHIT system must ensure that strong and substantial evidence is available to the recipient of the sender's identity, sufficient to prevent the sender from successfully denying having sent the data. This criterion includes the ability of a third party to verify the origin of the document.

Payor/Payer

Usually Third Party Payer: The public or private organization that is responsible for payment for healthcare expenses. Payers may be insurance companies or self-insured employers.

Personal Health Records (PHR)

An electronic application through which individuals can maintain and manage their health information (and that of others for whom they are authorized) in a private, secure, and confidential environment.

Health records maintained by an individual about him/herself or a member of his or her family.

Pharmacy Benefits Manager (PBM)

PBMs are third party administrators of prescription drug benefits

Provider

A hospital or doctor who "provides" care. A health plan, managed care company, or insurance carrier is not a healthcare provider. Those entities are called payers. The lines are blurred sometimes, however, when providers create or manage health plans. At that point, a provider is also a payer. A payer can be provider if the payer owns or manages providers, as with some staff model HMOs.

Public Key Infrastructure (PKI)

A structure under which a Certification Authority verifies the identity of applicants, issues, renews, and revokes digital certificates, maintains a registry of public keys, and maintains an up-to-date Certification Revocation List.

Private Key

The key of a key pair that is used to create a digital signature.

Public Key

The key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages (records or transactions) from the holder of the key pair.

Record Retention

Record retention requirements must be a minimum of 10 years. Presumably, patients would want their EHRs to be preserved forever since they represent patient medical history, but this would not be true for transactional/billing records. So law enforcement would need at a minimum, to replicate our current retention requirements for transactional records (that is, 10 years for civil enforcement purposes).

Reliability

Unique EHRs and the interoperable HIT system reliably and consistently do what they are supposed to do, perform as they are supposed to, use redundant or backup (of all transactions and changes) systems as necessary, and therefore are reliable. If the IT system fails, there is a goal of always having access to law enforcement and/all purposes available to information either redundant or backup.

Storage and Security

EHRs and/or data transmitted and retained in an interoperable HIT system must be stored and be secure from access by unauthorized and unidentified persons or users. This applies to data stored in the United States and offshore. Records must be retained; unaltered, readable, and retrievable and record retention must comply with all applicable laws and regulations. Records are to be readily available and in a readable format in the English language. Regardless of the physical location where the EHR is stored, the EHR must at all times be actually available, by legal process or as otherwise authorized by law, to patients, governmental and private payers, and law enforcement.

Traceability

This key critical principle relates to access and traceability. Access must be restricted (closed) to only approved, identifiable users. Collects and preserves all transaction (and/or clinical or encounter) information, including: Content or substance of the transaction (for example, the text of a contract or claim); The processing of the transaction (such as when and from where a communication was sent and when and where it was received throughout all phases of the transaction recordation/submission process); Identities of all parties or individuals involved in creating, transmitting and receiving the record or transaction and the identification of any changes those parties or individuals made to the record or transaction via the digital certificate and signature process referenced below.

The following references were used to compile this list of definitions:

LaTour, Kathleen and Eichenwald, Shirley, Health Information Management Concepts, Principles and Practice, AHIMA, 2002

www.ahima.org Body of Knowledge

www.whatis.com

www.aishealth.com/EhealthBusiness/EhealthTerms.html

http://www.advancedhealth.com/glossary

http://legal-dictionary.thefreedictionary.com

http://www.hhs.gov/healthit/glossary.html

http://www.cms.hhs.gov/glossary/

http://www.fairisaac.com/Fairisaac/Solutions/Enterprise+Decision+Management/Business+rule Fair Isaac Corporation 2005