FINAL REPORT

Recommended Requirements for Enhancing Data Quality in Electronic Health Record Systems

JUNE 2007

The Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services

Contract: HHSP233200600009T-233-02-0090 — Prepared by RTI International, RTI International is a trade name of Research Triangle Institute

May 2007

Recommended Requirements for Enhancing Data Quality in Electronic Health Records

Final Report

Prepared for

Kathleen H. Fyffe
Senior Advisor
The Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C Street SW, Room 4090
Switzer Building
Washington, DC 20201

Prepared by

RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

RTI Project Number 0208490.035.005

RTI Project Number
02008490.035.005

Recommended Requirements for Enhancing Data Quality in Electronic Health Records

Final Report

May 2007

Prepared for

Kathleen H. Fyffe
Senior Advisor
The Office of the National Coordinator
for Health Information Technology
U.S. Department of Health and Human Services
330 C Street SW, Room 4090
Switzer Building
Washington, DC 20201

Prepared by

RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

Contents

Figures

Tables

Executive Summary

ES.1 Introduction

The rising cost of health care has become a major issue in the United States. In 2005, the United States spent $1.98 trillion, or 16% of its gross domestic product (GDP), on health care. By 2016, health care expenditures are projected to surpass $4.1 trillion, or 19.6% of GDP.[1,2] In 2006, the National Coalition on Health Care (NCHC) noted that "inappropriate care, waste and fraud" were major contributors to the cost of medical care and health insurance.[3]

Electronic health record systems (EHR-S) are the key to the transformation of health care. EHR-S can

- improve the quality of care through enhanced evidence-based clinical decision support, the timely communication of clinical information, and better documentation;
- increase operational efficiency and contain costs by automating routine tasks, streamlining clinical workflow, and avoiding duplication of procedures;
- help collect data for uses other than clinical care, such as billing, quality reporting, disease surveillance, public health reporting, and fraud detection and deterrence;[4] and
- protect the privacy of health information through secure mechanisms and authorized access and control procedures.

Thus, widespread use of EHR-S has the potential to improve the quality of care, increase patient safety, reduce medical errors, and control health care costs. The notion that EHR-S can be leveraged in such a wide variety of ways is central to this project.

ES.2 Purpose and Objectives

The primary purpose of this project is to identify requirements for EHR-S that can help enhance data protections, such as increased data validity, accuracy and integrity including appropriate fraud management[*] which would prevent fraud[†] from occurring, as well as detect fraud both prospectively and retrospectively. A key component of creating these recommended requirements is to overlap whenever possible with those requirements currently in use for EHR certification. For example, authentication is required for privacy and confidentiality, but it is just as useful for preventing and detecting fraud. All of the requirements identified through this project are framed as recommendations to the industry.

The deliverables for this project are as follows:

1. A set of recommended requirements for EHR-S that will help prevent fraud from occurring, as well as detect fraud prospectively and retrospectively, with each requirement having an accompanying rationale

2. The identification of technical standards that will need to be harmonized so that the recommended requirements can be implemented in an interoperable fashion

3. A map between the anti-fraud requirements and certification criteria so that the recommended requirements can be ultimately embedded in certified EHR-S

4. Recommended next steps for education and research, as well as for implementing the anti-fraud requirements

While the focus of this project is on enhancing data accuracy, including the detection and prevention of fraud, it is important to emphasize the following points:

- By and large, clinicians are not engaged in fraudulent activities. Not all improper payments are the result of fraud, and not all unusual billing patterns are fraudulent. However, certain documentation practices, such as data errors, mistakes in coding, and confusion regarding billing codes and procedures may result in improper payments.

- The recommended requirements are aimed equally at reducing such erroneous documentation practices, preventing improper payments, and improving supporting documentation for legitimate claims submissions.

The transforming nature of EHR-S can benefit clinicians, patients, and payers by reducing human error and improper payment. EHR-S can also help detect and deter health care

[*] Fraud management is defined as the prevention, detection, and prosecution of fraud.

[†] For the purposes of this report, fraud is defined generally as a deliberately false representation of fact or a failure to disclose a fact that is material to a health care transaction. This includes but is not limited to deliberate submittal of false claims to private health insurance plans and/or tax-funded public health insurance programs such as Medicare and Medicaid. A more complete definition for health care fraud is in Appendix C.

fraud, protecting both clinicians and patients by documenting that correct procedures were used, highlighting outliers before they become serious issues, and giving patients a clearer understanding and peace of mind that their health records are being disclosed only to appropriately authorized users.

Although requirements that enhance data accuracy might overlap with current EHR certification criteria, thought must be given specifically to the criteria that will help combat both large- and small-scale suspected fraud, as well as accentuate the potential benefits of these systems with regard to reducing improper payment and human error. While a component of combating fraud is the ability to trace and audit information that may be used in prosecution, these same functionalities can be used to ensure information validity over time, which can protect both clinicians and patients. The ability to definitively show that correct procedures were used, use audit functionality as an "early warning system" to locate outliers before they become serious issues, or to provide patients with a clearer understanding and peace of mind that their records are being disclosed only to appropriately authorized users are all factors that can benefit all major stakeholders, from clinicians to patients to payers.

The Office of the National Coordinator for Health Information Technology (ONC) is responsible for overseeing activities that will realize the vision set by President George W. Bush in April 2004 to develop and implement a strategic plan to guide the nationwide implementation of interoperable HIT in both the public and private health care sectors. Through a series of initiatives, ONC has advanced this goal considerably over the past 3 years and continues to pave the way for HIT adoption across the country. In addition to moving the current directives forward, ONC is charged with planning for the future, such as anticipating the potential benefits of such a system. Designing enhanced data protections into EHR-S and the Nationwide Health Information Network (NHIN) has the potential to significantly reduce health care losses due to improper documentation and fraud.[4]

ES.3 Methodology and Rationale

In late 2006, ONC contracted with RTI International for a project involving three tasks: (1) develop recommendations for functional requirements for EHR-S that would enhance data by reducing the incidence of improper payment and assisting in fraud management, (2) validate the recommendations through public comment, and (3) work with appropriate HIT organizations to encourage adoption of the recommendations.

The basis for this project followed a subset of the 10 Guiding Principles[‡] outlined in the September 2005 *Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities* by the American Health Information Management

[‡] The 10 Guiding Principles are listed in Appendix B.

Association's (AHIMA's) Foundation of Research and Education (FORE).[4] First, the NHIN policies, procedures, and standards must proactively prevent, detect, and support prosecution of health care fraud rather than be neutral toward it. Second, 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 purposes. Third, data required from the NHIN for monitoring fraud and abuse must be derived from the NHIN's operations and must not require additional data transactions. In addition to these three principles, one of this project's important decisions was that fraud management requirements also can be used to improve the accuracy and quality of documentation for the large majority of clinicians who are not involved in fraudulent activity.

The project's first task involved the creation of the Model Requirements Executive Team (MRET), which brought together industry experts from various private and public stakeholder groups with multiple backgrounds in order to develop a set of recommendations for enhanced accuracy and fraud management requirements for Electronic Health Records (EHRs). The MRET worked in two groups, one that focused on prevention functions and another that focused on prospective and retrospective functions. Prevention functions are those that occur prior to and during the documentation process in an EHR. Prospective functions are those that occur after EHR documentation occurs but before a payment is made on any claim based on the EHR documentation. Retrospective functions are those that occur after a claim has been paid. Following the Guiding Principles outlined above, all requirements were constructed based on their ability to enable prevention of fraud management rather than remain neutral toward it, their ability to do this without impeding delivery of timely services to the patient, and to the extent possible, their ability to minimize EHR software programming and administrative costs associated with the recommended functions.

The next task validated the MRET recommendations through a public comment process by which the recommended requirements were released to the public using online tools to gather feedback from all interested parties. The majority of public comments fell into one of five categories:

- Ability to Detect or Deter Fraud
- Practicality of and Timeline of Implementation
- Cost Issues
- Burden and User Issues
- Patient and Privacy Issues

In response to the public comments, the MRET eliminated or modified requirements as necessary and developed a final set of recommendations for the requirements. These

requirements were supported by the vast majority of public responders and achieved high consensus among the members of the MRET.

Finally, the project staff worked closely with the leadership of the Health Information Technology and Security Standards Panel (HITSP) and the Certification Commission for Health Information Technology (CCHIT) to determine the most appropriate procedures for considering the recommended requirements in upcoming review cycles of each group. Each organization emphasized the importance of balancing the needs of enhancing accuracy, fraud management, and risk reductions that might enhance EHR-S against concerns that might inhibit EHR adoption. Productive conversations about both the costs and benefits of the recommended requirements led to feasible and actionable solutions that encouraged strong consideration within both groups.

ES.4 Recommendations

The recommended requirements for EHR-S developed herein provide the initial building blocks for increasing accuracy and fraud management within the health care system. Great efforts have been made to ensure the privacy and security of EHR data, but a deliberate effort to build these functional requirements into EHR-S and the NHIN could also increase data quality and reduce exposure to new and ever-evolving forms of electronically enabled health care fraud.[4]

This project produced 14 recommended functional requirements that, if included in EHR-S, would increase data accuracy and would aid in fraud management:

1. Audit Functions and Features
2. Provider Identification
3. User Access Authorization
4. Documentation Process Issues
5. Evaluation and Management (E&M) Coding
6. Proxy Authorship
7. Record Modification after Signature
8. Auditor Access to Patient Records
9. EHR Traceability
10. Patient Involvement in Anti-Fraud
11. Patient Identity-Proofing
12. Structured and Coded Data
13. Integrity of EHR Transmission
14. Accurate Linkage of Claims to Clinical Records

Each of these requirements was linked to current or planned CCHIT and Health Level 7 (HL7) criteria♦ where applicable. Twenty-two percent of the recommended requirements developed by the MRET map closely to existing CCHIT criteria. Another 45% of the requirements had some foundation in the current or planned criteria, but would require additions or modifications to support an active stance against fraud in EHR-S. Finally, 33% of the recommendations were found to have no match to current or planned criteria. These findings indicate that there is a significant base in current standards and certification requirements upon which to build proactive fraud management capabilities, but further work is required. Updating these current criteria would certainly provide a significant win for reducing costs associated with this current and growing problem.

The overwhelming majority of clinicians do not commit fraud and should not be burdened by mechanisms aimed solely at the few who do. Therefore, the recommended requirements also are directed at helping the majority, as they support quality of care through reduced errors and promote good documentation practices, as well as assist in fraud management, including protections against unmerited accusations of fraud and strengthened proofs of legitimacy. It is recommended that these requirements be considered among the many other improvements to be built into the emerging generation of EHR-S that are interoperable in the NHIN.

ES.5 Moving Forward

The activities undertaken in this project are simply the latest steps in an ongoing process to develop and integrate effective anti-fraud measures in the evolving HER-S requirements. Our efforts to date were constrained by time and resources and were not intended to produce a comprehensive solution to the fraud problem. Instead, our efforts are intended to raise awareness of the need to be proactive regarding the problems of fraud, rather than neutral or passive, and to encourage a dialogue between all parties interested in enhancing the accuracy of data in EHR-S.

At the conclusion of this project, the following suggestions are provided to ensure a continual, long-term approach to ensuring the integrity, validity, and accuracy of health record data. A full supporting explanation for each suggestion is provided in Chapter 5 of the report.

1: Current processes that are shaping the direction of HIT must be guided to advance health care information validity, accuracy, and integrity protections, including health care fraud management, in order to meet their future goals and objectives.

♦ The CCHIT roadmap establishes the areas of focus for the workgroups for future certification cycles by establishing future milestones.

1.1: ONC should include fraud management as one of its basic tenets in the next version of the Strategic Framework.

1.2: ONC must articulate the need to advance health information validity, accuracy, integrity, and fraud management functionalities to the American Health Information Community (AHIC) so that the appropriate use cases may be developed for HITSP and CCHIT.

1.3: Guidelines should be developed for both vendors and users of EHR-S regarding the appropriate use of documentation techniques to ensure complete, accurate, and quality documentation.

2: Given that this project narrowly focused on anti-fraud requirements for EHR-S; fraud management requirements for HIE/NHIN infrastructure and plans for their deployment should developed.

3: Greater efforts should be made to understand the concerns and opinions of all affected stakeholder groups regarding requirements that discourage fraud within EHR-S.

4: Further analysis is required to better quantify and characterize the current fraud activity as it relates to EHR-S, either as a tool for fraud or a potential source for fraud management. This should include an investigation into ways in which the appropriate entities in health care can work with law enforcement to communicate to providers how fraud schemes and fraud "rings" operate.

5: Stimulate advancements in the data aggregation process beyond the institutional level so that advanced analytics can detect trends and anomalies.

6: Increase consumer awareness of health care fraud and the role HIT, such as EHRs and PHRs, play in its reduction.

7: Educate health care stakeholders to a greater degree on the benefits of EHR-S containing requirements on health information validity, accuracy, and integrity and the impact these requirements will have on fraud management.

8: A designated position and supporting staff within ONC should be created to:

8.1 oversee and encourage the adoption of the recommended requirements developed under this project within CCHIT, HITSP, and other organizations responsible for the evolving NHIN;

8.2 develop future contracts to evolve and refine the functional requirements; and

8.3 oversee future research and analysis in this area.

1 Introduction

The rapid inflation of health care costs has become a major issue in the United States, although reaching consensus on how to control the problem has been elusive. Nevertheless, rising health care costs continue to affect families, employers, and health care workers across country. In 2006, the National Coalition on Health Care (NCHC) released a briefing that captured the gravity of this issue:[3]

- In 2004, the United States spent 16% of its gross domestic product (GDP) on health care. This percentage is projected to reach 20% by 2014.
- Health care spending is 4.3 times the amount spent on national defense.
- Premiums for employer-based health insurance rose by 7.7% in 2006.
- Since 2000, employment-based health insurance premiums have increased 87%, compared to cumulative inflation of 18% and cumulative wage growth of 20% during the same period.
- Almost 50% of the American public say they are very worried about having to pay more for their health care or health insurance, while 42% report they are very worried about not being able to afford health care services.
- One in four Americans say their family has had a problem paying for medical care during the past year.

In addition to issues of inefficiency, the NCHC (see Appendix C for a list of Acronyms and Definitions used throughout this report) review also noted the effects of "inappropriate care, waste and fraud" as major contributors to the cost of medical care and health insurance.[3] Widespread use of electronic health records (EHRs) has the potential to control health care costs and transform the U.S. health care system. Electronic Health Record Systems (EHR-S) can automate and streamline clinical work flows to help ensure all clinical information is communicated and to prevent delays in responses that result in gaps in care. Also, EHR-S can help in the collection of data for uses other than clinical care, such as billing,

management of quality of care, outcome reporting, public health disease surveillance and reporting, and fraud detection and deterrence.[4]

Issues of health care fraud have been a significant and growing concern for at least two decades. Since its foundation in 1985, the National Health Care Anti-Fraud Association (NHCAA) has focused on improving the private and public sectors' ability to detect, investigate, prosecute, and prevent fraud against private and public health insurance systems. In 2005, the United States spent $1.98 trillion, or 16% of its GDP, on health care.[1,2] These figures are projected to reach just over $4.1 trillion, or 19.6% of GDP by 2016. Although fraudulent claims are a small percentage of overall claims, they account for anywhere between 3% and 10% of total claim dollars.[5] Also, the adoption and use of EHRs across the country was estimated at 23.9% in 2005,[6] and the move toward EHR management systems provides an opportunity to proactively reduce billing errors and to mitigate fraud, allowing for the possibility of redirecting these funds to improve coverage and quality.

The transforming nature of EHR-S can benefit clinicians, patients, and payers by reducing human error and improper payment. EHR-S can also help detect and deter health care fraud, protecting both clinicians and patients by documenting that correct procedures were used, highlighting outliers before they become serious issues, and giving patients a clearer understanding and peace of mind that their health records are being disclosed only to appropriately authorized users.

2 Background and Context

This section provides background about the Office of the National Coordinator (ONC), its major initiatives, and a brief summary of the previous work conducted on issues of fraud in electronic health record systems.

2.1 ONC Formation and Major Initiatives

In January 2004, the president issued Executive Order 13335, which required the Secretary of the Department of Health and Human Services (HHS) to appoint a national coordinator for health information technology (HIT). The National Coordinator's role was to provide leadership for the development and nationwide implementation of an interoperable HIT infrastructure to improve the quality and efficiency of health care and, in particular, to reduce medical errors, lower costs, and provide better information for consumers and physicians. The president also called for health information to follow patients throughout their care in a seamless and secure manner.

In July 2004, the National Coordinator released a Framework for Strategic Action, which outlined 4 goals and 12 strategies to guide the development of a plan for national HIT adoption. The strong support for the framework created a unique opportunity to accelerate the nation's HIT agenda and will result in significant improvements in the quality, safety, and efficiency of health care and of individual and community health over the next decade.

ONC was officially established within the Office of the Secretary of HHS and formally announced in the Federal Register in August 2005. ONC was also designated as a separate HHS staff division and appropriation within the Office of the Secretary, with responsibility for its own operations.

In partnership with other government agencies, ONC issued a Request for Information (RFI) asking for input on how best to build, operate, and sustain a nationwide health information network to share clinical data in a secure and interoperable manner. The RFI drew more than 500 responses and the subsequent summary report was released to the public,

describing a broad set of initiatives necessary to support the implementation of HIT. ONC then began work to coordinate with public and private partners in the following areas:

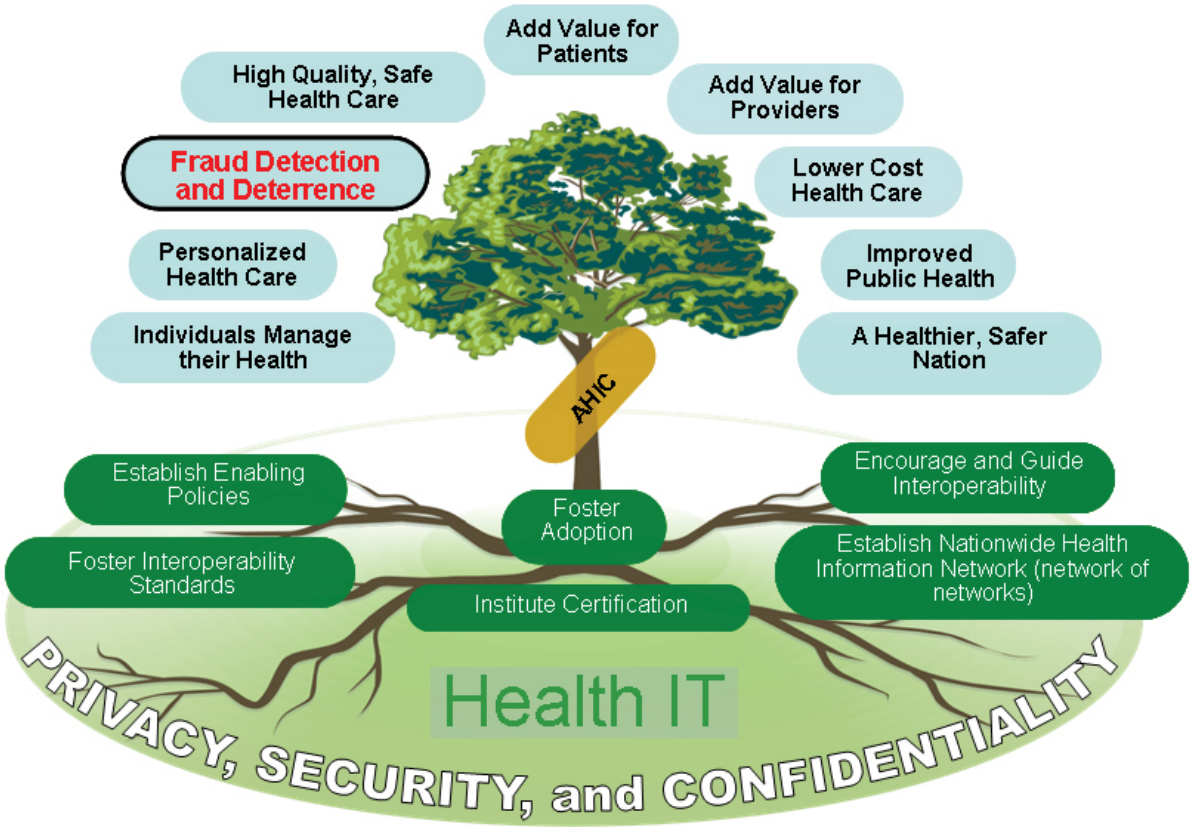
- Standards Harmonization—To evolve and evaluate a process to harmonize industry-wide HIT standards.
- Certification Commission for Health Care Information Technology—To develop and implement a certification process for EHR-S and health information exchange (HIE) networks.
- Privacy and Security—To evolve and advance plans to address variations in organization-level business policies and state laws related to privacy and security practices that might pose challenges to interoperable HIE.
- Nationwide Health Information Network (NHIN) Architecture—To evolve and evaluate prototypical NHIN architectures and advance capabilities for widespread HIE.
- Adoption of EHRs—To develop a standardized methodology to assess EHR adoption through surveys and studies.
- Hurricane Katrina Information Network and Digital Health Information Recovery Project—To plan and promote the widespread use of interoperable HIE in the Gulf Coast regions affected by recent hurricanes.
- Federal Health Architecture—An e-Gov Line of Business established in response to the President's Management Agenda. ONC provides leadership for define activities, collaborating with more than 20 federal agencies involved in health care.
- Interagency Health Information Technology Policy Council (i.e., the Policy Council)—To coordinate federal HIT policy decisions across federal agencies.

Figure 2-1 shows the areas currently supported by ONC in the effort to transform health care operations and the intended outcomes of these initiatives.

In 2005, Secretary Leavitt announced the formation of the American Health Information Community (AHIC), a national, public-private collaboration formed pursuant to the Federal Advisory Committee Act. The AHIC was established to facilitate the transition to interoperable electronic health systems in a smooth, market-led way and provides input and recommendations to the secretary. Membership consists of a combination of key leaders in the public and private sectors that represent stakeholder interests in advancing HIT. Approximately 10 meetings are held per year; members of the public have the opportunity to listen on the Web and participate during the public comment portion of each meeting.*

* Additional information can be found at http://www.hhs.gov/healthit/ahic.html.

Figure 2-1. HIT Support for Transforming Health Care



The AHIC initially established four workgroups that were charged with making recommendations for specific, achievable near-term results in the following areas:

- Biosurveillance—Transfer of standardized and anonymized health data from the point of health care delivery to authorized public health agencies within 24 hours of collection.
- Chronic Care—Secure messaging, as appropriate to health and care, as a means of communication between patients and the clinicians who care for them.
- Consumer Empowerment—Consumer-directed and secure electronic health care registration information and a medication history for patients.
- EHRs—Access by health professionals to current and historical laboratory results and interpretations that are standardized, widely available, and secure.

Additional AHIC workgroups have been formed recently to address confidentiality, privacy, and security; quality assessment and improvement; and the incorporation of personalized genomic information in health care.

Numerous approaches have been proposed to accelerate the adoption of HIT applications and make them interoperable. For this to occur, multiple stakeholders must be engaged and multiple issues and concerns must be resolved. Such a confluence, coupled with the

development of the necessary technological infrastructure, can lead to a true breakthrough of barriers that have precluded widespread implementation to date.

2.2 Health Care Anti-Fraud Initiatives

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

The objective of the second project was to study how the use of HIT could enhance and expand fraud management. For this 5-month field-based research project, FORE convened a cross-industry National Executive Committee (NEC) to identify the best opportunities to strengthen the fraud management capability of a nationwide interoperable HIT infrastructure. The NEC was made up of 22 cross-industry experts, including representatives of providers, payers, IT, fraud investigative services, finance, and government.

The major findings that emerged from the second contract were as follows[4]:

- Fraud in the health care context is defined by a number of legal authorities, but all definitions have common elements—a deliberately false representation of fact or a failure to disclose a fact that is material to a health care transaction, along with some damage to another party that reasonably relies on the misrepresentation or failure to disclose.
- The health care fraud problem is a serious and growing nationwide crime, linked directly to the nation's ever-increasing annual health care expenditures. In 2003, health care expenditures amounted to $1.7 trillion.[1] In that same year, it is estimated that losses due to fraud were 3% to 10% of the total amount of health care expenditures, or $51 billion to 170 billion.[5]
- Moving to an electronic environment without proactive fraud management capabilities built in has the potential to greatly increase fraud.
- While fraud management technology cannot eliminate fraud, it can significantly minimize fraud and abuse and ultimately reduce health care fraud losses.
- The use of advanced analytics software built into the NHIN is critical to fraud loss reduction.

2.3 Recommended Requirements: Project Purpose and Tasks

This project, based on guiding principles from AHIMA/FORE's 2005 project, involved development of recommended requirements for combating fraud and ultimately increasing the accuracy of EHRs:

- The NHIN policies, procedures, and standards must proactively prevent, detect, and support prosecution of health care fraud rather than be neutral toward it.

- 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 purposes.

- Data required from the NHIN for monitoring fraud and abuse must be derived from the NHIN's operations and must not require additional data transactions.

In 2006, ONC contracted with RTI to move forward with the development of a set of requirements that could be recommended as standards and eventually certification criteria within EHR-S. The key substantive tasks under this project included

- the creation of a set of recommended requirements and the release of these requirements for review and comment through a public validation process,

- working with members of the Health Information Technology and Security Standards Panel (HITSP) to engage support for the recommendations,

- working with members of the Certification Commission for Health Information Technology (CCHIT) to engage support for the recommendations, and

- the creation of supporting documents that would position fraud as a fundamental component of future standards and certification discussions.

Designing fraud management functionality into the NHIN has the potential to significantly reduce health care fraud losses.[4] Thought must be given specifically to the criteria that will help combat both large- and small-scale suspected fraud and also help accentuate the potential benefits of these systems with regard to reducing improper payment and human error. Many of the same functions that clinicians and patients rely on to assure the validity of information contained in a record can also be used to discourage improper payment and outright fraud. Thus, the key focus of the current project is to develop recommended requirements for EHR-S that would use functionalities present in the current EHR certification criteria and interoperability standards to continue to enhance data accuracy for the majority of providers seeking to provide quality care to their patients, and to make it more difficult to commit fraud in such systems. A summary of the tasks accomplished to meet this objective are highlighted below.

2.3.1 Task 1: Project Administration

The RTI team for this project included leading experts from RTI, AHIMA, and SPSS to ensure the necessary combination of subject matter expertise and management experience for successful project administration.

2.3.2 Task 2: Develop and Coordinate Recommended Requirements

RTI began the process of developing and coordinating the recommended functional requirements by first compiling a list of organizations whose leaders could provide input on the EHR requirements, as well as on the types of fraud that might flourish as EHR use

continues to rise. These individuals formed the Model Requirements Executive Team (MRET). Once the list was finalized, RTI project staff invited those included to participate in the MRET workgroup. (A complete list of the MRET members can be found in Appendix A). Those who agreed to participate took part in one of the following subgroups: the Preventive Subgroup or the Prospective/Retrospective Subgroup. Prevention functions are those that occur prior to and during the documentation process in an EHR. Prospective functions are those that occur after EHR documentation but before a payment is made on any claim, based on the EHR documentation. Retrospective functions are those that occur after a claim has been paid.

The purpose of the initial set of MRET and subgroup meetings was to produce a set of EHR-related fraud use case scenarios. From these use cases, a draft document was produced that outlined the proposed recommended requirements. The requirements were submitted to ONC leadership for their review and approval prior to public validation. Information gathered during the validation process was discussed among the two MRET subgroups and modifications were translated into the recommended requirements.

2.3.3 Task 3: Work with HITSP to Identify Existing and New Standards

RTI was charged with working with HITSP to identify existing and new standards. Core team members from RTI and AHIMA began connecting with HITSP early in the process to ensure that they were aware of the project progress and goals. All working materials and draft deliverables developed in Task 2 (upon approval for release by the MRET and the project director) were delivered to HITSP to ensure that (1) they were apprised of work in progress and (2) they were prepared to work with the RTI and AHIMA to identify a work plan for moving forward on appropriate standards once the final requirements were approved by ONC. The HITSP leadership, RTI staff, AHIMA staff, and ONC leadership worked collaboratively to identify the process that would move the recommended requirements forward.

2.3.4 Task 4: Work with CCHIT on Translating Recommended Functionalities and Requirements

RTI also was responsible for working with CCHIT to translate the recommendations into functional certification criteria. Compliance certification offers one way to ensure that anti-fraud requirements are implemented in EHR-S. As more and more EHR-S comply with certification criteria, it is important to consider the ability of anti-fraud functionality to discourage fraud in these systems. As with HITSP, certification is a lengthy process. Because CCHIT begins its process to develop and validate certification criteria 12 to 18 months before products are certified, it was especially important to keep CCHIT informed of the progress and direction of the recommended requirements.

Core team members from RTI and AHIMA began connecting with CCHIT early in the process to discuss objectives, time frames, and required deliverables for the project. All working materials and draft deliverables produced in Task 2 (upon approval for release by the MRET and the project director) were delivered to CCHIT leadership. This ensured that CCHIT was apprised of the work in progress and that they were prepared to work with RTI and AHIMA to identify a plan for considering certification criteria to meet the recommended requirements. The CCHIT leadership, RTI staff, AHIMA staff, and ONC leadership worked collaboratively to identify processes that would move the recommendations forward.

2.3.5 Task 5: Prepare Materials for CCHIT Workgroups

Finally, RTI was responsible for working with CCHIT to provide the appropriate materials to ensure the recommended anti-fraud requirements were submitted to the 2008 workgroups for consideration. AHIMA staff performed a thorough mapping of the recommendations to current CCHIT certification criteria and Health Level 7 (HL7) EHR-S conformance criteria. Those recommendations that did not match current criteria were discussed with CCHIT and determinations were made about which recommended requirements would need new certification criteria or modifications to existing criteria.

Members of AHIMA staff prepared the map described above and, along with RTI and the chair of the MRET, presented it in its various stages of development to CCHIT leadership. The result of these discussions was a plan and time frame to submit the map to CCHIT's 2007–2008 workgroups, who will be charged by the chair of CCHIT to appropriately consider adopting the requirements.

3 Research Activities

3.1 Creating the Model Requirements Executive Team and Developing Model Recommendations

The primary task under this contract was the development and coordination of a set of recommended functional requirements for EHRs. The purpose of these recommended requirements was to engage HIT infrastructure decision makers to consider health care fraud management in a proactive manner. In early October 2006, the project team began to identify individuals who could provide input into the creation of a single set of recommended requirements while representing the viewpoints of the stakeholders who would be affected by the recommended requirements. A list of individuals was supplied to ONC for approval. This list represented both federal agencies and private organizations, such as HIT vendors, clinicians, information management experts, quality improvement officers, and payer organizations. In late October, these individuals were formally invited to serve on the MRET. To maintain continuity and leverage the knowledge gained under the previous contracts, many members who served on the NEC were invited to join the MRET. One of the two co-chairs of the NEC chaired the MRET.

The charge of the MRET was to create a set of recommended requirements for EHRs, to help identify and mitigate fraud and proactively improve the quality and accuracy of documentation. A secondary goal was to develop requirements that can be delivered to HITSP for standards development and to CCHIT for certification criteria. To accomplish this goal, the MRET was divided into two major working groups: the Prevention Workgroup and the Prospective/Retrospective Workgroup. The charge of each group is described in the following sections.

3.1.1 Prevention Workgroup

This workgroup focused on requirements to detect and prevent inaccuracies and health care fraud, through inappropriate billing and up-coding prior to the creation of the EHR and during the documentation process that occurs in an ambulatory setting. Evidence suggests that potential health care fraud can occur at the time of the seminal record event and, therefore, the creation point may exist before the physical embodiment of a record.

Members of this workgroup were asked to develop requirements focused on preventing either errant or deliberately illegitimate record creation and/or enabling appropriate audit documentation when necessary, as well as the requirements for the preclinical record documentation phase. This group was tasked with covering subjects including, but not limited to, the following:

- IT infrastructure: Accountability, access and availability, traceability, auditable, identification, authentication, nonrepudiation, integrity (nonalterability after finalization), storage and security, record retention, reliability, signatures and encryption keys
- Documentation process (EHR application software): Record completeness, corroborating data, use of defaults, finalization, billing code generation
- Patient ability to review clinical records
- Education and publicity

3.1.2 Retrospective/Prospective Workgroup

This workgroup focused on requirements to detect, investigate, and prevent improper payments after the clinical documentation in the EHR has been created (before and after payment). This group was charged with considering two components. First, retrospective detection of improper payment will require investigation and prosecution to recover losses. Second, improper payment will sometimes be detected at the time of claim submission, prior to claim payment, and will initiate investigation. Subjects considered by the group included, but were not limited to, the following:

- Claim review and adjudication phase: Access to clinical documentation and corroborating data, record locator system access, fraud pattern templates derived from data mining and rules
- Identification of abnormal claims patterns, which could include predefined outliers or abnormalities, such as an unusually high frequency of seemingly replicated data, using advanced analytic software at the patient, provider, and institutional/organizational levels

The workgroups met on a regular basis throughout November and December. All workgroup meetings were attended by the MRET chair to provide continuity, as well as by members of the AHIMA team, including the AHIMA liaison to the MRET. For more information on the process undertaken by each of the workgroups, please see Appendix D. Throughout the process, it was understood that anti-fraud requirements had a likelihood of sparking intense discussion from multiple stakeholders. There were a number of requirements offered for discussion that were not further pursued because it was believed that consensus could not be achieved.

In mid-December, the MRET met as a group to determine the final set of recommended functional requirements that would be submitted to ONC for review and that would be released for public comment through an online validation process (described in detail below). Requirements were accepted or rejected on the basis of an open, transparent public comment process, and many were edited after thorough discussion. Although there were concerns voiced regarding some of the requirements, the overwhelming majority of MRET members approved each individual requirement set forth in the final submission. Section 5 Results provides a detailed listing of these requirements, along with their rationale statements.

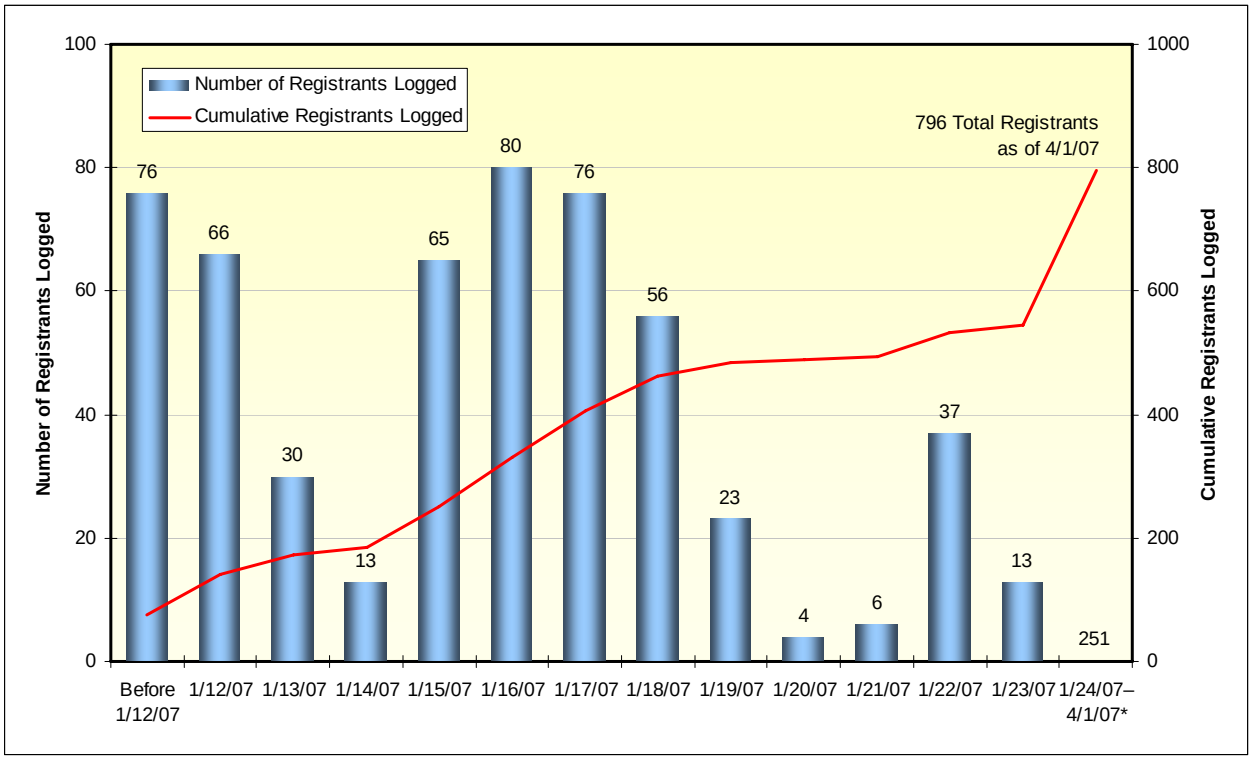
3.2 Public Validation Process

An essential component of creating a meaningful set of requirements included undertaking a public validation process. This process of gathering input from various stakeholders was intended to provide a "reality check" in the formulation of the final set of recommended requirements. Originally, RTI proposed convening a small number of public forums and gathering input from attendees at meetings such as the American Medical Informatics Association and National Association of Health Data Organizations. As the project progressed, however, it became clear that broader stakeholder input could be gathered by releasing the MRET draft requirements and creating a mechanism for capturing feedback online. For detailed information on the tools and processes used to collect this data, please see Appendix E.

Although the period of time allotted for the collection of public comments was fairly short because of a rigorous project schedule, every attempt was made to notify all interested stakeholders of the impending review in advance. Because of the early notification efforts, the site logged 76 user registrations prior to releasing the anti-fraud recommendations document on January 11, 2007. Those that preregistered received an e-mail notification that the draft requirements were available for their review, and another press release continued to generate interest. In all, nearly 800 users registered with the site to gain access to the recommended requirements. ***Figure 3-1*** shows the distribution of registrants over the life of the project.

More than 500 of those individuals had registered by the time the public comment data were collected and distributed to the members of the MRET for review prior to an all-day, in-person meeting held in Washington, D.C., to determine the final set of recommended functional requirements that would be recommended under this contract. A total of 75 individuals or organizations accessed and supplied data within the Public Comment module. While individual names were withheld from the MRET on the basis of confidentiality, organization names (31 total) were provided as an important component in understanding the context of the comments. ***Table 3-1*** provides a list of the organizations supplying

Figure 3-1. Distribution of Registrants to Recommended Requirements Web Site



Note: No public comments were collected for consideration by the MRET after January 24, 2007.

Table 3-1. Organizations Providing Public Comment

American Health Information Management Association	Georgia Hospital Association
Fox Systems Inc.	Transaction Security, Inc.
American Association of People With Disabilities (AAPD)	Substance Abuse & Mental Health Services Administration
ASA, LLC	University of Pittsburgh Medical Center
CPSI	Preferred Family Health Care, Inc.
Blue Cross/Blue Shield Association	Synergistic Office Solutions, Inc.
American College of Physicians	AHIMA EHR Practice Council
California Office of HIPAA Implementation	Evanston Northwestern Health Care
American Academy of Family Physicians	ANAKAM
Home Care Association of NYS	BIOMPI, LLC
Spectracom Corporation	New Jersey Hospital Association
Omnicare Information Solutions	Medical Esolutions
National Association for the Support of Long-Term Care	Medical Informatics Subcommittee of the American College of Physicians
AG Research	CentrifyHealth
ADENA Health System	National Association for the Support of Long-Term Care

American Hospital Association

comments during the public comment period. ***Table 3-2*** provides a list of affiliations indicated by both individuals and organizations that reported at the beginning of the Public Comment module.

Table 3-2. Self-Reported Affiliations Provided for Public Comment Respondents

Stakeholder Affiliation	Response	Percentage
Consumer or patient	13	17.33
Health care purchaser	9	12.00
Quality improvement organization	9	12.00
Informatics specialist	6	8.00
Blank[a]	6	8.00
Physician	5	6.67
Health care payer	4	5.33
Government agency	2	2.67
Safety net provider	1	1.33
Standards organization	1	1.33
Other	19	25.33
Other	0	0.00
HIT vendor	0	0.00
Public health agency	0	0.00
Clinical research	0	0.00%
Total	**75**	**100.00%**

[a]Response was not provided for affiliation.

The full set of recommendations appears later in this report and represents only those requirements that achieved support from a majority of the public responders and very high consensus among members of the MRET. A full discussion regarding the findings of the public comment data also appears later in this report. However, it is important to note that of the 14 requirements released for validation, all received at least 65% acceptance[*] within the public comments. A large number of the comments involved suggestions on rewording or clarifying the particular requirement and did not involve a significant change in the purpose or intent. The maximum number of "No" votes received for any single requirement was 18 out of 66 responses.

The public comment process not only collected information from a wide variety of stakeholders, it also provided insight into the level of acceptance that these stakeholders have for the requirements. Furthermore, the comments highlighted some gaps in stakeholder consensus, as well as the steps recommended to move this work forward.

[*] Acceptance is deemed as a "Yes, support" vote or a "Could support" vote.

3.3 Work with HITSP and CCHIT

Following the creation of the recommended functional requirements, an equally important set of activities was undertaken with both the HITSP and the CCHIT. Project staff, headed by a team from AHIMA, worked closely with each organization to determine what steps could be agreed on to move the anti-fraud work forward. Both HITSP and CCHIT were contacted prior to the release of draft recommendations to discuss the project and were encouraged to provide comments on the requirements. These comments, along with the public comments, were taken into consideration to produce a final document.

For HITSP, a plan was outlined to provide candid feedback on the recommendations indicating whether each was already included in the current standards or roadmap standards or whether gaps exist in standards that would require a new directive to investigate. Additionally, project staff worked with HITSP leadership to produce a plan that would adequately move each recommendation forward as necessary and on its own timeline.

Project staff, led by the AHIMA team, also worked with CCHIT leadership not only to confirm the mapping, but also to lay out a plan to incorporate those requirements that did not currently exist in the CCHIT criteria, if it was seen fit to do so in the future. This included the production of a plan that would produce appropriate documentation for the 2008 CCHIT workgroups, the details of which are discussed below.

These activities were approached with the utmost diligence to ensure that the anti-fraud recommendations put forth under this work moved to the next step. The production of the recommended requirements was not enough, on its own, to ensure that the discussion about anti-fraud would move ahead. Although issues of security and privacy have been exceedingly important in both the standards' harmonization and gap analysis performed by HITSP, as well as to the certification requirements formulated by CCHIT, fraud management is not a current direct mandate of either of these organizations. The limited extent that there is overlap between the MRET recommendations and current or proposed CCHIT requirements is due to the overlap between privacy and security functions and fraud management functions rather than a focus on fraud management per se. Through the public comment process undertaken by this project, some insight can be provided into the reasons that consensus around the issue of fraud management has been somewhat difficult to attain.

Nevertheless, fraud is happening in both paper- and electronic-based systems. EHR-S provide a new opportunity for fraudulent behavior, and on ever-increasing scales, although they also provide opportunities to discourage those that would use these systems for personal gain. Development of common standards and regulations that increase accuracy and discourage fraud has the potential to make the health care system more efficient,

specifically with respect to the increasing adoption of electronic systems. The exact cost of not developing these types of standards and regulations is unknown, although every effort should be made to strengthen the efficiencies and cost saving capabilities of EHR-S for the long-term benefit of the health care system.

4 Results

Through a series of workgroup meetings, the MRET constructed a list of recommended functional requirements that relate to the following topics:

1. Audit Functions and Features
2. Provider Identification
3. User Access Authorization
4. Documentation Process Issues
5. Evaluation and Management (E&M) Coding
6. Proxy Authorship
7. Record Modification after Signature
8. Auditor Access to Patient Record
9. EHR Traceability
10. Patient Involvement in Anti-Fraud
11. Patient Identity-Proofing
12. Structured and Coded Data
13. Integrity of EHR Transmission
14. Accurate Linkage of Claims to Clinical Records

This chapter outlines these recommended requirements in detail and also provides additional information regarding the results of activities leading up to and following the creation of the requirements. The next section discusses the information collected from the public comment and provides context for the final list of recommendations set forth under this contract.

4.1 Public Comment Findings

As mentioned earlier, the draft requirements were provided for public comment, reflecting an acute awareness that any recommendations put forth under this contract would require broad-based consent. While these comments led to important discussions, and in many cases updates to the requirements, they also provided invaluable insight into the issues that stakeholders are likely to point to as EHR fraud management evolves.

Public comments on the draft requirements generally fell into one of five categories:

1. Ability to Detect or Deter Fraud
2. Practicality of Implementation and Timeline Issues
3. Cost Issues
4. Burden and User Issues
5. Patient and Privacy Issues

The remainder of the comments largely voiced requests for clarification of key terms, which were addressed in preparing the final requirements.

As shown in ***Figure 4-1***, the majority of reviewers supported each of the final requirements. Comments that were more substantive than editorial typically were offered when there was disagreement with the way a requirement was stated or with the implications it might have. Most comments were related to specific requirements, although on occasion there were comments about the endeavor itself. An overview of the comments for each of the categories listed above is provided in this section. Specific comment excerpts by category can be found in Appendix F.

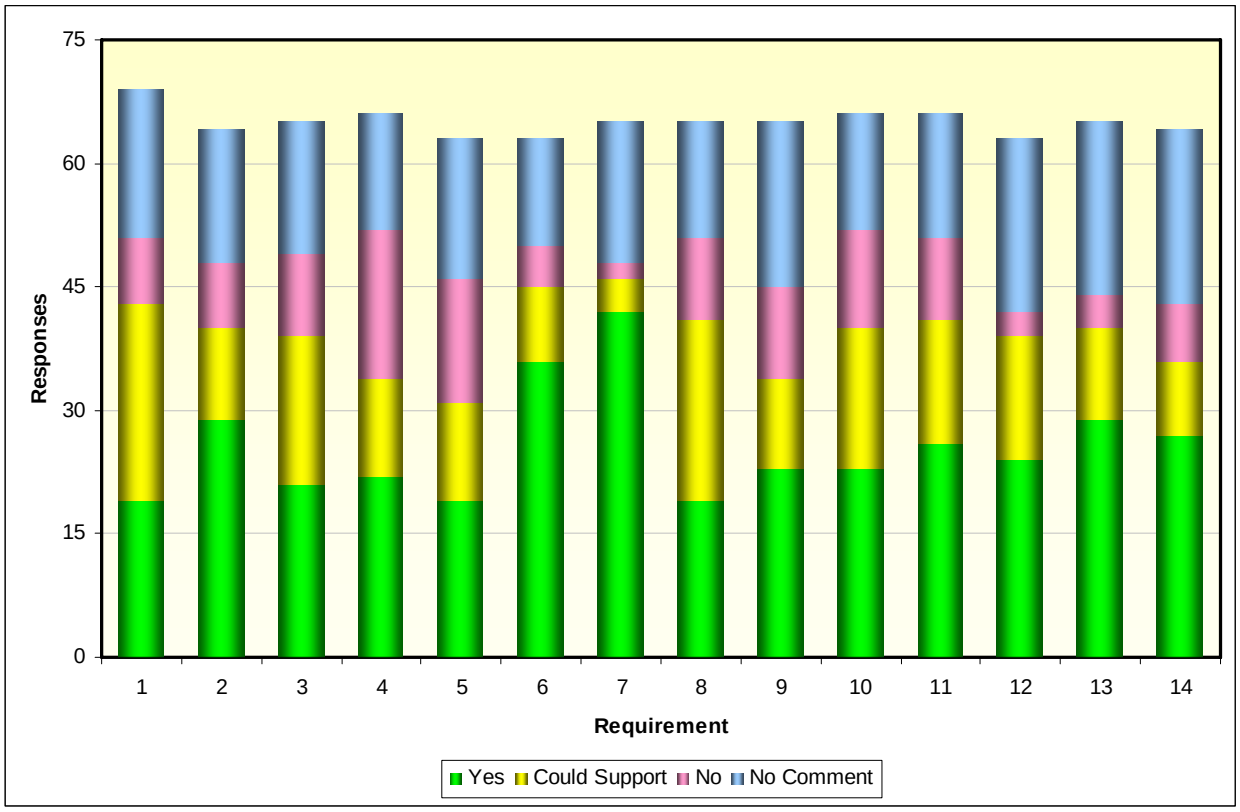
4.1.1 Ability to Detect or Deter Fraud

Most reviewers expressed support for the requirements as effective tools for deterring and detecting fraud, while others noted concern about their efficacy and relevance. One supportive reviewer noted that some of the requirements "provide a critical first step towards correcting significant compliance and quality care inadequacies in these systems." However, another felt that the requirements contained "very little" of what should be part of EHR standards geared toward reducing fraud. Two other reviewers suggested using post-processing techniques to identify fraud. Finally, some public reviewers who expressed concern that specific requirements or elements of requirements were not directly related to fraud detection suggested other areas where they may be relevant.

The comments supplied indicate general support for combating fraud in electronic HIE systems, but convey that the recommendations provided were either too weak or too broad to effectively detect or deter improper payment. In response to these issues, the MRET revised many of the requirements to indicate more specific detail and provided additional

rationale to indicate how the recommendation would specifically aid fraud management in EHR-S.

Figure 4-1. Public Comment Results, by Recommendation



4.1.2 Practicality of Implementation and Timeline Issues

Many reviewers commented on the practicality of the requirements and feasibility of implementation within the timelines supplied. Some were concerned with the burden for the developers and programmers, while others questioned whether the requirements proposed were realistic considering the technology available to date. When technology was not in question, many reviewers still noted concerns regarding the suggested implementation dates.

The MRET team had a clear understanding of the technical issues that were associated with the recommendations, and experts from both SPSS and SAS were included in discussions during the creation and finalization of the requirements. The consensus was that the technical capacity of EHR programs would have to expand as these systems transition to become the primary mode of data storage and transfer. Although these capabilities may not be realized fully for many years, the importance of creating systems today that can handle

the needs of tomorrow is of high importance when discussing deterrence and detection of fraud.

4.1.3 Cost Issues

Many public reviewers expressed concern about the cost of implementing the draft requirements; many felt that it was not clear who would be responsible for the development, systems, and training costs associated with the requirements. One reviewer noted that "the development costs, and hence the provider acquisition costs, for the proposed requirements are quite substantial." Other reviewers were concerned that cost and complexity issues would discourage the use of EHRs.

In fact, cost is a real issue preventing the adoption of EHRs today. The MRET recognized the need to use current criteria as the basis for its recommendations whenever possible to reduce the development costs associated with requiring new criteria. The intention of each individual requirement was to ensure that the high levels of waste due to fraud and inaccuracies would be reduced, not accelerated, as the experts predict, as EHR-S are adopted. Therefore, only requirements that the MRET agreed would be of the highest benefit for reaching this goal were included in the final set of recommended model requirements.

4.1.4 Burden and User Issues

In addition to the comments related to cost, some reviewers also expressed concerns regarding the effect of the draft requirements on user productivity. Some commented that there is a need to "gain a better understanding of the burden placed upon users" if certain requirements are adopted, while others stated outright that the burden would be too great. One concerned reviewer suggested that the added burden could lead to delayed adoption or non-adoption, while another advocated for "end-user simplicity and eliminating the need for hardware installation on the end-user device."

There was a concerted effort on the part of the MRET to reduce rather than increase complexity. Again, instructing the workgroups to use the current CCHIT criteria as a guide led to the production of requirements that attempted to harmonize with these criteria rather than disrupt them. In addition, there was consensus among the MRET that all recommendations put forward in the final document could become valuable tools for users who are concerned about maintaining records that are less susceptible to fraud. Providing specific, real-time guidance concerning common mistakes and inaccuracies in an EHR-S could ultimately improve the workflow process and create more accurate records in the long-term.

4.1.5 Patient and Privacy Issues

Many reviewers expressed concerns regarding patient privacy and the acceptable level of access to records for patients, doctors, and payers. Some reviewers noted that they could only support certain requirements if patient privacy concerns were addressed directly, and one felt "little to no attention or recognition" was given to patient concerns and rights in the draft requirements. Another reviewer noted, "How much data the payor should obtain in order to make a payment is truly the only question that needs to be answered as pertains to EHR standards."

The basis of many of the MRET recommendations can be mapped to current privacy and security criteria required by the Health Insurance Portability and Accountability Act (HIPAA) Security Rule[§] and supported by HITSP standards and CCHIT criteria. Because the HIPAA Privacy Rule allows for the disclosure of personal health information (PHI) without the individual's signed authorization for purposes of treatment, payment, and health care operations,[**] special consideration must be given to scenarios involving some level of access by groups other than the primary user, such as patients themselves, visiting physicians, and payers.[††] Because these disclosures are permissible, EHR-S must be adequately prepared to handle them appropriately to ensure that each user is allowed access only to the information necessary for each unique encounter. Leaving these encounters unregulated as they become increasingly frequent in EHR-S would be disastrous for privacy and security, as well as for the incidence of deliberate fraud.

4.2 Final Recommended Requirements for EHR-S

The major task undertaken for this contract was the creation of a set of functional requirements that aims to combat fraudulent activity in EHR-S. Although the methods for creating these recommendations have been outlined earlier in this report, it is important to note that significant changes were made to the draft requirements after taking the public comment data into account, in an effort to produce requirements that would be capable of producing a significant level of consensus moving forward. Of the recommendations included in this document, all were supported by a significant majority of MRET members; in many cases, the support was unanimous.

After submission of this initial set of requirements to ONC, the recommendations underwent a second series of revisions. It was essential to project staff to ensure that each requirement was appropriate and feasible with respect to the current climate. The intent of

[§] 45 CFR 164.308 requires a covered entity to conduct a risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI.

[**] 45 CFR 164.501: Health Care operations include "the conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs."

[††] See CFR 45 164.506 (c)(4)(ii), which mentions "health care fraud and abuse detection or compliance."

the recommendations was to create requirements that would fit within existing criteria whenever possible, but also would raise awareness of the need to include issues of enhancing accuracy and discouraging improper payment as a distinct and essential consideration when creating EHR standards and certification criteria. Therefore, an extraordinary amount of care went into assuring the applicability of the final set of requirements to multiple clinical settings, such as hospitals, physician offices, home health care organizations, nursing homes, and managed care organizations. Significant consideration was also given to providing the flexibility to harmonize the final requirements with future EHR capabilities.

Below is a summary of each of the final functional requirements produced under this contract and agreed upon by the MRET majority, project staff, and ONC. Following each requirement is a rationale statement that provides important context for the recommendation and why it is believed to be imperative to discouraging fraud in EHR-S.

4.2.1 Requirement 1: Audit Functions and Features

4.2.1.1 Requirement 1A: Audit Functions and Features—Audit Log Content

1.1 Require a standardized audit log that supports both security risk management and fraud management.

- 1.1.1 Date/time/user stamp for each clinical entry at data element level or some other suitable mechanism to allow assessment of the number of user operations used to create an encounter note or encounter note update.
- 1.1.2 Date/time/user stamp of each access to the EHR.
- 1.1.3 Date/time/user stamp of "signature event" (whether proactive or auto default) for encounter or progress notes.
- 1.1.4 Date/time of release of encounter or progress note for administrative/billing process or, alternatively, date/time billing transaction was created based on encounter or progress note.
- 1.1.5 Minimum data to be captured in the audit log includes the following:
  - 1.1.5.1 Access type (i.e., creating, editing, viewing, printing, or electronically transferring all or any part of the patient record)
  - 1.1.5.2 User ID, including National Provider Identifier (NPI) number if available, of person accessing the record
  - 1.1.5.3 Location or logical address from which the information was accessed
  - 1.1.5.4 Date and time that the information was accessed using NTP/SNTP synchronized time
  - 1.1.5.5 For printing or transferring electronically all or parts of a record that is initiated by a user, reason for transaction entered by user

Rationale:

A comprehensive fraud management program, which encompasses the prevention, detection, and prosecution of health care fraud, requires efforts at multiple levels, most of which occur outside of the EHR. For fraud that involves the creation of fraudulent claims based on clinical services provided to patients, the EHR in all of its aspects is central to fraud management in important ways.

- For prevention, the mere fact of knowing that information is being collected on the process and content of clinical documentation that could be used to detect fraudulent behavior in itself serves as a deterrent to that behavior. Audit reports provide the tools to self-monitor and apply preventive strategies before detection or prosecution.

The audit log provides the who, what, when, where, why, and how in this cycle. This log is central to prevention, detection, and preservation of key evidence to support prosecution of health care fraud.

4.2.1.2 Requirement 1B: Audit Functions and Features—Audit Log Operation

1.1.6	The audit log will be operational whenever the system is available for updates or viewing of the clinical record. There may be exceptional circumstances for technical or other reasons when this cannot occur:
1.1.6.1	If the system supports a user command to disable or enable the audit log, such command shall be limited to roles associated with users that administer the system.
1.1.6.2	All user commands that enable or disable the audit log shall be recorded in the audit log as auditable events.
1.1.6.3	If the system is accepting updates at a time when the audit log is impaired or disabled, a notification of the occurrence of this state will be made available to the system administrator.
1.1.6.4	The audit log shall support a means of unequivocally determining if it contains gaps when users updated the record while the audit log was not being recorded, even if the audit log was not recorded for a reason other than explicit disablement by a user. Such determination shall be evident solely by examining the audit log.
1.1.7	Deletions or alteration of the contents of the audit log will not be allowed by users.
1.1.8	System must support a user-friendly output version of the audit log for transmission, printing, or export, which shows all details of events described in 1.1.1–1.1.5 above.

Rationale:

Much of fraud detection revolves around analyzing patterns of information available in claims and other databases that raise the suspicion of fraudulent behavior for further investigation. The more detailed information available to these pattern-detection systems, the greater the ability to differentiate legitimate from fraudulent behavior.

When a suspicious pattern, which would be pre-determined based upon historical analysis of similar data, is detected, the ability to reconstruct further detail regarding the who, what, when, where, why, and how of clinical documentation provides the tools for investigation. Furthermore, when fraud is detected, these same tools can be used for prosecution.

The continuing iterative process above enables not only the creation of prospective screening tools to prevent payment of fraudulent claims, but allows evolution of those tools as the perpetrators of fraud become increasingly sophisticated in their methods. Some of these preventive measures can be built into the EHR-S themselves to prevent the creation of fraudulent documentation.

4.2.1.3 Requirement 1C: Audit Functions and Features—Audit Support

1.2 Audit Support Function: Require documentation of the audit support functionality in the vendor provided user guides and other support documentation, including how to identify and retrospectively reconstruct all data elements in the audit log including date, time and method of entry.

1.3 The system shall have the capacity to allow authorized entities to read only access according to agreed upon uses and only as a part of an identified audit subject to appropriate authentication, authorization, and access control procedures. Such access shall also be subject to appropriate release of information protocols, local audit policies, minimum necessary criteria, and other contractual arrangements and, laws, and:

- 1.3.1 Require “auditor” be a supported class of user
- 1.3.2 Limit access to pertinent functions and views only for portions of audit logs covered by the audit.
- 1.3.3 Access remains controlled by the facility and the same authentication and audit supports would apply.
- 1.3.4 Remote access may be offered if agreed to by the clinical data organization subject to the aforementioned protocols and suitable authentication

1.4 Data and Document Retention, Disposal and Archiving: Retain all EHR-S data and clinical documents (including audit logs) for the time periods designated by the EHR system owner’s policies or legal requirements. Audit logs should be retained as long as clinical records. Provide the ability to destroy, deactivate, or archive EHR data/records in a systematic way according to the EHR system owner’s policies and after legally-prescribed retention periods.

Rationale:

We are cognizant of the issues surrounding the requirements for audit functionality and recommend alternatives to the following questions:

1. Will the process of creating and maintaining the audit log impair the performance of the EHR system? If this is the case, we do not recommend its implementation in all aspects (1a-1c), but rather a phase-in of as much as possible over time, without interfering with performance. Some vendors are able to do all of this now, while others can do little. It will be the task of certification organizations such as CCHIT to determine the appropriate timing for specific implementation certification criteria.

2. Will access to this level of detail by authorized entities involved in fraud management pose a problem for privacy of patients or violate physicians' rights? The risk exists that system capabilities for such access, if used inappropriately, could pose a problem. Therefore, we recommend that this access be strictly limited according to all levels of law, policy, and local practice.
3. Will this add too much cost to EHR-S? It will add some cost, as do most modifications to software. However, with appropriate design, we believe that the added costs can be minimized to levels that are cost-effective for EHR-S. Stakeholders should also consider the trade-off gains from preventing losses to fraud through prepayment deterrence and corrections of possible billing errors and recovering dollars from improper payments compared to losses that would continue to be incurred if the recommended functionality is not implemented.
4. Is this appropriate for all clinical settings? We recommend that it first be applied in the ambulatory area and then modifications be made, as necessary, as requirements are developed for other settings.

4.2.2 Requirement 2: Provider Identification

2.	EHR-S must support the use of the National Provider Identifier (NPI)* in the EHR audit log to identify the individual provider, or, in situations when an NPI is not available for an individual, a single unique internal provider identifier is assigned.

Rationale:

A commonly known fraud scheme is for fraud perpetrators to steal provider identifiers and use them to submit false claims. Use of the NPI in EHR-S and claims may significantly reduce fraud losses. The NPI is required for electronic claims, beginning May 2007 for large health care providers and May 2008 for small health care providers.[7]

Use of the NPI also would enable payers to only remit claims payments to registered providers at their registered locations, further reducing the motivation for provider identity theft. Furthermore, to investigate health care fraud, it is necessary to have either the NPI or a unique internal provider ID attached to all transactions in the EHR for inclusion in all EHR transaction logs. This requirement documents the author of an entry into an EHR.

4.2.3 Requirement 3: User Access Authentication

3.1	Demonstrate the ability to support user ID/strong password in 2008.
3.2	Demonstrate the ability to evolve the level of user authentication in the future, as industry standards require.

Rationale:

Fraud prevention is enabled by requiring user authentication to the EHR. The health care entity bears responsibility for ensuring that all individuals authorized to access the EHR have the requisite credentials for the services they provide. Validation of the process of credentialing in the EHR will allow matching of the provider profile to the type of services billed.

The National Committee on Vital and Health Statistics and CCHIT both have released roadmap documents that speak to proposed authentication technology requirements. Both entities have expressed a requirement for a user ID/strong password by 2008. In the case of the CCHIT roadmap, these requirements include public key infrastructure (PKI) and enhanced authentication as goals for 2009 and beyond. Instead of outlining specific recommendations concerning the level of authentication requirements, this recommendation endorses these roadmaps and encourages the continual technological growth of advanced authentication practices in EHR-S.

4.2.4 Requirement 4: Documentation Process Issues

4.	System will provide the capability to produce a business version of each encounter note or progress note which indicates:
4.1	Date/time/user stamp for each entry
4.2	The methods used in the creation of the entry including but not limited to:
4.2.1	Direct entry via integrated hardware keyboard or mouse
4.2.2	Speech recognition
4.2.3	Automated, machine-entered default information
4.2.4	Pre-created documentation via form or template
4.2.5	Copy/import of an object including date/time user stamp of original author
4.2.6	Copy forward previous note contents including date/time user stamp of original author
4.2.7	Dictation/ Transcription
4.2.8	Import from an external system
4.3	If a copy of the encounter note is required or desired to accompany a claim, provide the ability to submit the business version.

Rationale:

EHRs provide a variety of tools that enable a provider to be more efficient when documenting an encounter, from voice recognition to simple copy and paste procedures. Likewise, EHR tools provide payers, employers, and other entities opportunities for efficiency when following up on an encounter and contributing to the generation of any PHI on a patient. These tools include the use of defaults, templates, copying, and others. These are legitimate benefits of using an automated system and can be extremely helpful if used correctly; however, the tools can also open the EHR-S up to fraud or abuse. The intent here is not specifically to encourage auditing or monitoring of encounter notes, which would have

only a limited effect on proactive fraud monitoring. The use of copy/paste, default forward, and/or import functions is left to the discretion of the user of the EHR-S, although specific warnings regarding the use of these tools by different payers may be a consideration. However, having an audit version of the EHR that shows the tools used and the individuals who used them can enable retroactive detection of patterns of abuse or fraud.

4.2.5 Requirement 5: Evaluation and Management (E&M) Coding

5.1	The system shall be capable of prompting for omitted necessary administrative data or codes. This could include the capability to prompt a physician if the selected E&M code is not consistent with the documentation in the encounter note.
5.2	Prompts that are driven by E&M administrative processes shall not explicitly or implicitly direct a user to add documentation. This does not apply to prompts for additional documentation for E&M levels already achieved, for medical necessity or for quality guidelines/clinical decision support.

Rationale:

This is new wording for CCHIT requirement 237 of the ambulatory functional requirements, which states, "The system shall prompt for data required to determine appropriate administrative (evaluation and management) codes if such data is not present in encounter data." It is appropriate for EHR-S to calculate an E&M code from the encounter data that has been entered and to indicate the basis for that calculation. However, it is not appropriate to suggest to the provider that certain additional data, if entered, would increase the level of the E&M code, nor is it appropriate for the payer to have auto-adjudicated down-coding based on similar coding logic without a data-generated basis. The wording of the current CCHIT requirement, although unintended, could be interpreted as allowing for these situations.

It is also well documented that E&M codes can vary significantly from one individual coder to another without any ill intention. Underlying this requirement should be an understanding that these inconsistencies in and of themselves are not an indicator of fraud, and that record analysis must be able to account for variances. The use of a prompt merely alerts the individual providing the code of possible inconsistency and thereby may become an extremely helpful tool to provide some consistent guidance to clinicians.

4.2.6 Requirement 6: Proxy Authorship

6.1	Retain date/time/user stamp of original data entry person when data entered "on behalf" of another author.
6.2	If an assistant is used to enter data that will subsequently be signed by a provider, retain the date/time/use stamp of the data entry person as well as the provider.

Rationale:

A provider's staff can obtain information from a patient and put the information into the clinical record, or the provider can obtain the information from a patient and have the staff

record the information on his/her behalf. It is important to be able to distinguish which of these mechanisms, if either, was used and by whom.

4.2.7 Requirement 7: Record Modification after Signature

7.	Require retention of original documents and any amendments after "signature event" (including automatic "closing" of record). Any updates after signature event must be handled as amendments.

Rationale:

At some point when documenting an encounter, the documentation cannot be altered without an audit trail of the original entry. Typically, this is when the provider signs a note electronically or when a practice automatically closes an encounter at some specified time period after the encounter. Retaining an audit trail of changes after this event prevents subsequent fraudulent alteration of the record.

4.2.8 Requirement 8: Auditor Access to Patient Record

8.	The system shall have the capacity to allow authorized entities read-only access to the EHR according to agreed upon uses and only as a part of an identified audit subject to appropriate authentication, authorization, and access control functionality. Such access controls shall also support the applicable release of information protocols, local audit policies, minimum necessary criteria, and other contractual arrangements and, laws, and:
8.1	Require "auditor" be a supported class of user
8.2	Limit access to pertinent functions and views only for patient records covered by the audit.
8.3	Access remains controlled by the facility and the same authentication and audit supports would apply.
8.4	Remote access may be offered if agreed to by the organization subject to the aforementioned protocols and suitable authentication
8.5	Demonstrate the ability to provide a paper copy of such information in the event access to the EHR is not possible.

Rationale:

Detection of a fraudulent claim is often difficult when a payer has access only to EHR information for a single encounter. Reviewing information over an entire episode of care for a single patient allows greater ability to detect fraud. Such access should be subject to appropriate protocols for release of information, local audit policies, minimum necessary criteria, contractual requirements, federal and state laws, and applicable contractual agreements between the provider organization and the payer.

4.2.9 Requirement 9: EHR Traceability

9.1	Demonstrate the ability to generate and embed a document ID tracking number for patient chart outputs or exports, unique for each instance when a patient chart output/document is printed, electronically communicated, or otherwise exported from the EHR:
9.1.1	Display tracking number on printed document (regardless of the document format including, but not be limited to .doc, .pdf, etc. and attach to electronic copy.
9.1.2	Tracking number audit record should contain user creating document, date/time, and an option to include the reason for printing or transferring an electronic copy of the document
9.1.3	Tracking number function requirement also applies to transfers of information from the EHR system to a billing system where these are separate or otherwise independently functioning systems.
9.1.4	Maintain an audit log of tracking numbers in a file that is treated as a business record of the organization.

Rationale:

It is typically easier and more credible to create a fraudulent claim by using real patient record information than attempting to fabricate this information de novo. Preventing the unauthorized transfer, printing, and viewing of patient records reduces the ability to obtain such information.

The principle is already well established that electronic documents include mandatory data field contents embedded specifically for the purpose of tracking; however, there is still debate about standards for displaying and printing this information. Understanding that there needs to be a process for producing printed copies of documentation on an ad hoc basis for several purposes, including ordinary disclosure accountability, the suggestion that a certified EHR would disable the “print screen” function or other methods of printing a hard copy of any portion of the clinical record except through predefined software-driven processes, is an attempt to ensure that the adequate information to track the hard copy record is automatically appended and a tracking number is printed either to the hard copy or to the electronic version of the file.

Requirement 9 also assumes that the EHR system’s ability to track documentation events will support the reconstruction of how the export was created and thereby allow reconstruction and audit of its contents when necessary.

4.2.10 Requirement 10: Patient Involvement in Anti-Fraud

10.1	Allow patient access to his or her own completed records and release of information (disclosure) log, as required by law or agreed to by the clinical provider.
10.2	Demonstrate the ability to capture patient comments in the EHR.

Rationale:

Patients can be a potent force in combating fraud. However, they must be given the tools to do so. This is one purpose of an Explanation of Benefits notification from a claim. Access to and review of the medical record documentation that was used to generate a claim would be an even stronger tool for prevention and detection of fraud. Allowing patients to comment when they are reviewing portions of their records gives them an opportunity to point out potential errors or potentially fraudulent documentation.

4.2.11 Requirement 11: Patient Identify-Proofing

11. Require capability to document/record that identity-proofing was completed and the method used to verify (i.e., check photo id, prior relationship, or verification of information an individual knows or can produce) consistent with the recommendations of the Confidentiality/Privacy/Security Workgroup of the American Health Information Community.

Rationale:

One of the fastest growing types of health care fraud is medical identity theft—patients commit fraud by masquerading as another individual in order to obtain medical services. Once detected, the consequences and potential liability for this type of fraud can be costly, as noted in the examples below:

- Provider organizations will be left with unbillable services for the fraudulent individual (or a payer requesting reimbursement for services provided to the fraudster).
- Individuals will have incorrect information in their medical and billing record, which could negatively affect them in the future (e.g., when obtaining services such as life or health insurance, obtaining equipment or a device in which insurance will only pay once in a lifetime).
- Payers reimburse for services not delivered to the insured.

To reduce the risk of medical identity theft to all parties, positive identification of an individual prior to delivery of services is crucial. The Confidentiality/Privacy/Security workgroup of the AHIC has identified this as a critical issue and, at the January 23, 2007, meeting offered its recommendations on handling identity-proofing. The workgroup defined identity-proofing as the process of providing sufficient information to correctly and accurately establish and verify a patient's identity to be used in an electronic environment. The workgroup outlined three ways identity-proofing can be completed: (1) by validating a government-issued picture ID; (2) by establishing a durable relationship; or (3) by verifying identity based on information an individual or designated proxy knows or can produce, such as an address, date of birth, current or last prescription, and other verifying information.

4.2.12 Requirement 12: Structured and Coded Data

12.1	The EHR system must have the ability to accept structured and coded data for existing data standards.
12.2	Support directly capturing clinical information from the clinician in structured and coded form to the maximum degree possible consistent with the principle of not adversely impacting user productivity.

Rationale:

Use of advanced analytics and pattern detection is one of the strongest tools to prevent fraudulent behavior. The greater the degree of coding in a record, the greater the ability to prevent fraud.

4.2.13 Requirement 13: Integrity of EHR Transmission

13.	Transmit clinical information to other information systems using standards that retain the available level of coding and structure, such as the HL7 Clinical Data Architecture.

Rationale:

Intentional or unintentional modification of records can occur during the transfer from one system to another. Systems must be able to irrefutably ensure that transmission of EHR information has occurred in an unaltered state.

4.2.14 Requirement 14: Accurate Linkage of Claims to Clinical Records

14.	Require a traceable and auditable path from a claim payment or a transmission of a pay for performance payment to the clinical documentation supporting it.
14.1	Information transmitted to a claims preparation system will include the Document ID tracking number generated in the EHR traceability requirement above.
14.2	All information transmitted for the purposes of supporting claims or pay for performance payments will be logged in an audit file that cannot subsequently be changed by a user or administrator of the EHR system. The audit file will include the time at which the submission was created and any relevant document ID tracking numbers generated under the EHR traceability requirement above.

Rationale:

The ability to link a claim to the clinical record on which it is based is a fundamental requirement for fraud detection. Systems must be able to irrefutably ensure the linkage of a claim to the clinical record on which it is based. It is essential to be able to trace back to the original clinical encounter documentation that was used to generate the claim, regardless of whether or not the EHR system is integrated with the claims-generating system.

4.3 Mapping of MRET Requirements to CCHIT Criteria

In preparation for Tasks 3, 4 and 5, the MRET anti-fraud EHR system requirements were mapped to the 2006 CCHIT criteria for ambulatory care EHR-S. The mapping identified three categories under which the anti-fraud requirements could be grouped: (1) those already

addressed in existing CCHIT criteria; (2) those partially addressed by existing criteria or standards; and (3) those not addressed by existing criteria, resulting in new requirements that would need to be written.

The mapping and identification of gaps or differences between the MRET anti-fraud requirements and CCHIT certification criteria provided a foundation for discussions with HITSP (Task 3) and CCHIT (Task 4). Specifically, the mapping of anti-fraud requirements to both CCHIT certification criteria and HL7 EHR-S conformance criteria was necessary for the following reasons:

- A direct match between an anti-fraud requirement and a CCHIT certification criterion could enable CCHIT to consider incorporating such anti-fraud requirements immediately as part of its current and roadmap certification requirements.

- CCHIT certification criteria is congruent with the format of the HL7 EHR-S functional model. Indeed, many of the certification criteria developed by CCHIT were submitted to HL7 and were subsequently included in the latter's EHR-S functional model. In a bidirectional manner, many of the HL7 EHR-S conformance criteria were adopted by CCHIT for their certification criteria, and there are many other HL7 conformance criteria that could be adopted by CCHIT for their roadmap. Thus, if there was an anti-fraud requirement for which there was no or only a partial match with CCHIT's certification criteria, then it may have been possible to complete the match by extracting criteria from the HL7 model. These criteria could then be recommended to CCHIT for their consideration.

- Anti-fraud requirements for which there were no corresponding CCHIT certification or HL7 EHR-S conformance criteria either indicated a gap in certification or the EHR-S standard—in which case the anti-fraud requirements suggested future enhancements to both. Alternatively, it may have indicated that the mission and purpose of neither certification compliance nor the EHR-S standard covered that aspect of anti-fraud, and the gap was acceptable.

Once gaps or differences were identified, language was proposed to modify existing criteria to incorporate anti-fraud concepts. When there was not an existing CCHIT criterion to directly or partially match an anti-fraud requirement, one was drafted as suggested language for CCHIT and HITSP consideration.

Appendix G illustrates the results of the mapping process. Each of the 14 anti-fraud requirements was broken down into testable criteria. The 2006 CCHIT criteria for ambulatory care were reviewed for a match to the MRET recommendations. Matches or partial matches were documented, as were no matches.

- **Match**: A match indicated that the entire concept from the MRET requirement was captured by a CCHIT criterion and the intent could be met fully.

- **Partial Match**: Partial matches were much more subjective and varied widely—in general only a portion of a MRET requirement was met in a CCHIT criterion or else the intent of the anti-fraud/fraud management concept was not captured. For

example, CCHIT indicated that audit logging processes are completed for security purposes only. The audit criteria could be used for anti-fraud purposes as well as security. Suggestions were made to expand the purposes to include anti-fraud.

- **No Match**: No match was found between the concept or MRET requirement and the existing CCHIT criteria.

Suggested language was drafted for CCHIT to adapt existing criteria that were partial or no matches. In drafting language, the HL7 EHR-S functional model standard also was reviewed. If there was a conformance criterion in the HL7 standard that addressed a gap in CCHIT, it was documented in Appendix G. Whenever possible, HL7 was used for suggested language to address the gaps between the MRET and CCHIT; however, there were only a few instances in which this occurred.

Of the 55 unique EHR system testable anti-fraud criteria derived from the original 14 MRET requirements, the mapping process indicated that there was not always a one-to-one match between an MRET requirement and a CCHIT criterion (in some cases, more than one CCHIT criterion was identified to address an anti-fraud criterion). ***Table 4-2*** provides a summary of the matches, partial matches, and no matches.

Table 4-2. Number of Matches between MRET Requirements and CCHIT Criteria

Type	Number	Percentage
Match	12	22
Partial match	25	45
No match	18	33

The process is subjective based on the reviewers' interpretation of the MRET requirements and CCHIT criteria. Public comments from CCHIT identified the applicable function and were used to assist in the mapping process.

4.4 Outcomes of HITSP and CCHIT Objectives

The final task under this contract required working with both HITSP and CCHIT leadership to develop a plan moving the recommended anti-fraud model requirements forward within the respective groups. The intent was not to circumvent the structure or processes put in place by either entity but to engage them in an understanding of the importance of the health care fraud issue and to ensure that all work products provided the best opportunity possible for consideration and inclusion into the standard processes.

4.4.1 HITSP Plan Moving Forward

RTI supplied HITSP leadership with a final draft recommended requirements document. HITSP leadership reviewed the document to comment on which draft model requirements

already fit within the HITSP Interoperability 1.0 Specification and which do not. Five of the MRET recommended requirements (User Access Authentication, Proxy Authorship, Auditor Access to Patient Record, Structured and Coded Data, and Integrity of EHR Transmission) were found to have sufficient basis in the current standards. For those draft model requirements that were not included the current standards, HITSP leadership worked with RTI to determine whether (a) the recommended requirement is close enough to an existing standard that it can be assigned for consideration to either the Privacy and Security Workgroup or the Foundations Workgroup or (b) for those that were outside the current HITSP scope, what actions, if any, would allow for a full standards' gathering and harmonization process.

Requirements assigned to workgroups for future consideration (group [a]) included Audit, Documentation Process Issues, Provider Identification, EHR Traceability, Patient Involvement, and Patient Identity-Proofing. Three other requirements were considered outside the current scope (group [b]), including E&M Coding, Record Modification after Signature, and Accurate Linkage of Claims to Clinical Records. Of these three, only the last could feasibly be covered by an increase in scope, because the first two deal with basic functional standards of EHR-S, which is outside the HITSP mandate to harmonize interoperability standards. If a use case covering Accurate Linkage of Claims to Clinical Records was developed in the future, however, and provided to HITSP by the AHIC as a future official use case, a full standards' harmonization and gap analysis could occur.

4.4.2 CCHIT Plan Moving Forward

RTI's subcontractor, AHIMA, worked closely with CCHIT to develop the final mapping and recommendations document. CCHIT leadership reviewed the document to determine whether the suggested wording for the partial matches was appropriate for submission to the workgroups. For those requirements that provided partial or no matches to the existing criteria, CCHIT determined which workgroup(s) would be most likely to consider the updated/new criteria for the 2008 cycle. RTI produced an evidence document to submit to each workgroup, along with the mapping and suggested revisions to ensure that a strong case will be made for inclusion and that counterpoints can be answered during the process.

5 A Discussion about Moving Forward

The continual support for EHR adoption nationwide provides a significant opportunity for new advancements in quality provided to the patient and monetary benefits for all stakeholders. This project developed recommendations for EHR functional requirements necessary for an active response to increase prevention and detection of human error and improper payment and to discourage fraud in ways that are not possible in a paper-based system. These recommendations provide an opportunity to increase the safety and security of EHR-S, improve their overall quality, and reduce their likelihood of providing an open opportunity for fraud.

The suggestions for moving forward, provided below, are driven by the following underlying issues.

1. Patient safety and quality improvement are rightfully the primary areas of focus for HIT initiatives. Health care fraud shares with these a fundamental concern for the protection and improvement of the validity, accuracy, and integrity of health care information.
2. Fraud continues to be a major area of concern for those involved in health care, resulting in the continual loss of billions of health care dollars if left unchecked. Unless proactive steps are built into the NHIN from the start, the potential is great for this problem to increase.
3. Given the extent to which the recommended requirements for EHR-S can be implemented over time and harmonized to support existing requirements, significant health care dollars could be captured and reinvested in the health care system.
4. At the policy level, fraud management must continue to be a focus for the industry, along with patient safety; security and confidentiality of patient information; quality improvement; and broad considerations of validity, accuracy, and integrity of all health care information.

In order to ensure that issues of accuracy, quality, improper payment, and fraud in EHR-S continues to grow in their importance as part of the nationwide discussion surrounding the safety of EHR systems, the following recommendations should be implemented.

1: Current processes that are shaping the direction of HIT must be guided to advance health care information validity, accuracy, and integrity protections, including health care fraud management, in their future goals and objectives.

1.1: ONC should include fraud management as one of its basic tenets in the next version of the Strategic Framework. Including fraud management as a specific concern in the Strategic Framework will send a clear signal to the health care industry of the importance of fraud management alongside quality improvement, patient safety, privacy, and security. In addition, inclusion in the Strategic Framework can help explain how health information validity, accuracy, and integrity required for security, privacy, confidentiality, and quality of care have simultaneous benefits for fraud management. Lastly, inclusion will emphasize that implementing fraud management is a leveraged, not a new effort, which can help recover dollars lost to fraud while improving the quality of care.

1.2: ONC must articulate the need to advance health information validity, accuracy, integrity, and fraud management functionalities to AHIC so that the appropriate use cases may be developed for HITSP and CCHIT. As previously noted, fraud management currently is not a mandate for HITSP or CCHIT, although an increased focus should also be a part of future NHIN initiatives. Including data integrity and fraud management in future AHIC use cases, or developing use cases that deal specifically with these issues, will provide the mandate for standards' harmonization, certification compliance, and activities undertaken toward construction of the NHIN.

1.3: Guidelines should be developed for both vendors and users of EHR-S regarding the appropriate use of documentation techniques to ensure complete, accurate, and quality documentation. Mandate the minimum criteria necessary to ensure that EHR-S are maintained to facilitate accurate record keeping and ongoing fraud management programs.

2: Because this project narrowly focused on anti-fraud requirements for EHR-S, fraud management requirements for HIE/NHIN infrastructure and plans for their deployment should be developed.

Guidelines and requirements can be developed through the use case process, as in Recommendation 1 above. They also could be done as a separate study, or they could be built in as contractual requirements in future NHIN/HIE requests for proposals.

Nationwide HIE plans should contain specific time frames for the varying levels of the NHIN's interoperability and its integration with and implementation of advanced analytics software for aggregate data analysis. The plans should also minimize the period of automated transactions without interoperability across providers and move to a NHIN with

analytic tools applied to aggregate data as quickly as possible once interoperability is achieved (see Recommendation 5). Time frames should be developed for the following:

- Development of enterprise management and operating policies for all stakeholders so that HIEs can support activities that encourage enhanced data accuracy and health care fraud management
- Part of the HIE infrastructure standards, procedures, and prototypes to facilitate increased accuracy and health care fraud management
- Development of HIE 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 data accuracy and health care fraud management
- Assessment of the feasibility of creating a Healthcare Information Sharing and Analysis Center as a component of a national fraud management program that would work in concert with the NHIN entities.

3: Greater efforts should be made to understand the concerns and opinions of all affected stakeholder groups regarding requirements that discourage fraud within EHR-S.

A small but important percentage of stakeholders responding to the recommendations remain uncomfortable with the inclusion of fraud management requirements into the current standards and certification criteria. Tied to the fundamental Guiding Principles articulated in the previous ONC contract, those building EHR-S and the NHIN must be proactive rather than neutral toward fraud management. Although this may lead to differences as to how to be proactive, efforts to understand their concerns and opinions must be included as part of any efforts to move forward and help resolve these differences.

A thorough study should have appropriate components to definitively capture the root of their concerns and provide actionable solutions to determine best practices for reaching and maintaining consensus.

The purpose of instituting fraud management requirements is not to make EHR-S more complex for the majority of honest users, but to provide greater quality and accuracy in their documentation, in addition to safeguarding them from fraud and, perhaps more importantly, from instances of improper payment or human error.

An official network of providers who have successfully adopted an EHR-S should be assembled to provide input for those who are interested but concerned about the functionality of these systems. A network of users that can attest to the positive effect such functions have had on their practice could be a significant method for encouraging consensus.

There remains both controversy and confusion regarding the appropriateness of certain efficiency and time-saving features of existing EHR-S. To what extent should default values be used and in what circumstances? What is the appropriate role of copy/paste functions in documentation? What is appropriate decision support regarding financial and billing functions, charge capture, and E&M code calculation? These and other questions deserve discussion among all stakeholders and the development of clear guidelines.

4: Further analysis is required to better quantify and characterize the current fraud activity as it relates to EHR-S either as a tool for fraud or a potential source for fraud management. This should include an investigation into ways in which the appropriate entities in health care can work with law enforcement to communicate to providers how fraud schemes and fraud "rings" operate.

The data available to the MRET during this process were incomplete or unavailable for review. To the extent that detailed quantified information is already present within the Department of Justice, CMS, and other federal organizations, as well as private payer organizations, these data should be better summarized and made available to future ONC-related efforts. It is likely, however, that further research and analysis is required to develop this information. Such information as the number of audits performed on practices and the specific findings of those audits as they related to fraud should be documented. Comparisons of quality, documentation error, fraud activity, and costs, including E&M code levels, should be compared between practices that do and do not use EHR-S. Efforts are needed to quantify the effects, both positive and negative, of various EHR operations, including defaults, copy/paste, decision support rules, and other common features and functions of EHR-S.

5: Stimulate advancements in the data aggregation process beyond the institutional level so that advanced analytics can detect trends and anomalies.

Coupled with the data that may already be available (see Recommendation 4), the recommended fraud management requirements will generate data that must be aggregated and analyzed. Data aggregation can reasonably be conducted at the institutional level because an organization can aggregate and analyze its own data. However, as has been pointed out in this report, fraud occurs well beyond the walls of a single institution. Thus, it is necessary to aggregate data beyond the institutional level. To that end, the process to identify appropriate entities and policies, as well as the technical network architecture and infrastructure to aggregate data, should be developed.

6: Increase consumer awareness of health care fraud and the role HIT, such as EHRs and PHRs, play in its reduction.

A consumer awareness program should be developed and deployed on the role of information technology in health care fraud and its ability to detect and assist consumers in personally minimizing fraud. The program also should emphasize the benefits of the NHIN and EHRs in the national fight against health care fraud in program content and publications.

7: Educate health care stakeholders to a greater degree on the benefits of EHR-S containing requirements on health information validity, accuracy, and integrity and their effect on fraud management.

Such education should disseminate definitions and guidelines to inform and address the impact and consequences of health care fraud on the economy, on patient health risk, and on population heath risk, and should inform stakeholders of the interpretation of health care fraud guidelines with regard to EHR documentation and coding.

8: A designated position and supporting staff within ONC should be created to

- oversee and encourage the adoption of the recommended requirements developed under this project within CCHIT, HITSP, and other organizations responsible for the evolving NHIN;
- develop future contracts to evolve and refine the functional requirements; and
- oversee future research and analysis in this area (see Recommendation 4).

References

1. Centers for Medicare & Medicaid Services (CMS). "National Health Expenditures Aggregate, Per Capita Amounts, Percent Distribution, and Average Annual Percent Growth, by Source of Funds: Selected Calendar Years 1960-2005." and Baltimore, MD: Department of the Treasury, the Office of the Chief Actuary, Social Security Administration, and the Office of the Actuary, Centers for Medicare and Medicaid Services. As accessed May 18, 2007, from http://www.cms.hhs.gov/NationalHealthExpendData/.

2. Centers for Medicare & Medicaid Services (CMS). "National Health Expenditure Projections 2006-2016." Baltimore, MD: Department of the Treasury, the Office of the Chief Actuary, Social Security Administration, and the Office of the Actuary, Centers for Medicare and Medicaid Services. As accessed May 18, 2007, from http://www.cms.hhs.gov/NationalHealthExpendData/.

3. National Coalition on Health Care (NCHC) (2007). Health Insurance Cost: Facts on the Cost of Health Care. Washington, DC: National Coalition on Health Care. <http://www.nchc.org/facts/cost.shtml>.

4. Foundation of Research and Education, American Health Information Management Association (FORE, AHIMA) (2005). *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. Chicago, IL: Foundation of Research and Education, American Health Information Management Association. <http://www.hhs.gov/healthit/ documents/ReportOnTheUse.pdf>.

5. National Health Care Anti-fraud Association (NHCAA). About Health Care Fraud. Washington, DC: National Coalition on Health Care. <http://www.nhcaa.org/ about_health_care_fraud>. Accessed on May 17, 2007.

6. Jha, A.K., Ferris, T.G., Donelan, K., DesRoches, C., Shields, A., Rosenbaum, S., et al. (2006). "How Common Are Electronic Health Records in the United States?" *Health Affairs* 25(6): w496-w507.

7. Centers for Medicare & Medicaid Services (CMS). "Guidance on Compliance with the HIPAA National Provider Identifier (NPI) Rule: After the May 23, 2007, Implementation Deadline." As accessed May 18 2007, <http://www.cms.hhs.gov/NationalProvIdentStand/ Downloads/NPI_Contingency.pdf>.

Appendix A: MRET Membership

Model Requirements Executive Team (MRET)

Donald W. Simborg, MD, MRET Chairman

Susan Hanson, MBA, RHIA, FAHIMA, Executive Coordinator

Preventive Workgroup

Reed Gelzer, MD, MPH, CCHC **Workgroup Chairman*	Advocates for Documentation Integrity and Compliance
Robert Burleigh, CHBME	Brandywine Healthcare Services
Rebecca S. Busch, RN, MBA, CCM, CBM	Medical Business Associates, Inc.
Jamie Ferguson	Kaiser Permanente
Lawrence Hughes, JD	American Hospital Association
Holly Louie, CHBME, BSN	Practice Management, Inc.
Matthew McMullen, PhD, JD	Centers for Medicaid & Medicare Services
Blackford Middleton, MD, MPH, MSc	Partner's HealthCare Systems, Inc.
Wes Rishel	Gartner Group
Susan Turney, MD, MS, FACP, FACMPE	Wisconsin Medical Society

Retrospective/Prospective Workgroup

A. John Blair, III, MD **Workgroup Chairman*	Taconic IPA, Inc.
Rebecca S. Busch, RN, MBA, CCM, CBM	Medical Business Associates, Inc.

Bonnie Cassidy, MPA, RHIA, FAHIMA	Cherry, Bekaert & Holland, LLP
Christopher Dorn	United Health Group/Ingenix
Byron Hollis, Esq., CFE, AHFI	Blue Cross/Blue Shield of America
Richard Ingraham	SAS US Commercial
Holly Louie, CHBME, BSN	Practice Management, Inc.
Matthew McMullen, PhD, JD	Centers for Medicaid & Medicare Services
Louis Saccocio	National Health Care Anti-Fraud Association
James Speros, JD	Veterans Health Administration
Alan Yuspeh, JD, MBA	Hospital Corporation of America

Project Staff

Colleen McCue, PhD Project Director	RTI International
Stephanie Rizk, MS Project Manager	RTI International
Linda Dimitropoulos, PhD Senior Advisor	RTI International
Joe Murphy Analysis Task Leader	RTI International
Nicole Horstmann Project Coordinator	RTI International
Don T. Mon, PhD HITSP and CCHIT Liaison	American Health Information Management Association
Michelle Dougherty, RHIA Requirements Mapping Task Leader	American Health Information Management Association
Kathy Giannangelo	American Health Information Management Association
Susan Stellmacher Technical Consultant	SPSS
Jean Jenkins Technical Consultant	SPSS
Terry Taerum, PhD Technical Consultant	SPSS
Jodi Blomberg Technical Consultant	SAS

Appendix B: Guiding Principles from 2005 FORE/ AHIMA Contract

1. **NHIN policies, procedures, and standards must proactively prevent, detect, and support prosecution of health care fraud rather than be neutral to it.** ‡‡

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.

3. A standard minimum definition of a legal health record (LHR) must be adopted for EHRs.

4. Comprehensive health care fraud management programs must enable rather than inhibit national EHR adoption.

5. Healthcare fraud management is the responsibility of all health care stakeholders.

6. Increased consumer awareness of health care fraud and the role HIT and EHRs play in its reduction can improve the effectiveness of health care fraud management programs.

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 purposes.**

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 health care fraud management programs.

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.

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

Source: FORE/AHIMA Contract HHSP23320054100EC, September 30, 2005.

‡‡ Principles in bold indicate those that were the focus of this work.

Appendix C: Acronym Guide and Definitions of Terms

AHIC	American Health Information Community (aka, “the Community”)
AHIMA	American Health Information Management Association
CCHIT	Certification Commission for Health Information Technology
FORE	Foundation of Research Education
EHR	Electronic Health Record
EHR-S	Electronic Health Record System
HFMA	Healthcare Financial Management Association
HIE	Health Information Exchange
HIT	Health Information Technology
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITSP	Health Information Technology Standards Panel
HL7	Health Level 7
MRET	Model Requirements Executive Team

NCHC	National Coalition on Health Care
NEC	National Executive Committee
NHCAA	National Health Care Anti-Fraud Association
NHIN	National Health Information Network
ONC	Office of the National Coordinator for Health Information Technology

C.1 Definitions

Abuse—A range of the following improper behaviors or billing practices including, but not limited to, billing for a noncovered service, misusing codes on the claim (i.e., 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 requiring user IDs and passwords. Access control can be based on roles, status of a situation (e.g., 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, mandatory access control, discretionary access control, time-of-day access control, classification access control, and subject-object separation.

Adjudication—Processing claims according to a contract.

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

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 the user's actions. An audit trail is mandated by HIPAA regulation for patients' medical information.

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 can do so reliably and without alteration.

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 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; and the subject's signature and date.

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 are 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.

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 health care provider. A legal and ethical concept that establishes the health care provider's responsibility for protecting health records and other personal and private information from unauthorized use or disclosure.

Deidentified—Under the HIPAA Privacy Rule, data are deidentified 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 do not include any of the following 18 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 older than 89); telephone numbers, fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, and account numbers; certificate/license numbers; vehicle identifiers, including license plate numbers, device identifiers, and serial numbers; URLs; Internet protocol addresses; biometric identifiers; full-face photos 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 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 ensures 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 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 health care entities to implement this technology derives from the need for medical outcome studies, efficient care, fast 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.

Encryption—Software coding procedure to prevent hacking or illegal accessing by unauthorized persons. 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.

Explanation of Benefits—The statement the beneficiary receives after a patient files a claim with the insurance company or a claim has been filed on the patient's behalf by the doctor. This statement is a summary of the action taken on the claim—how much of the bill was paid by the third–party payer/insurance company and how much is the patient's responsibility to pay (even though this portion may have been paid at the time of service).

Fraud (Health Care)—For the purposes of this report, fraud is defined generally as a deliberately false representation of fact or a failure to disclose a fact that is material to a health care transaction. This includes but is not limited to deliberate submittal of false claims to private health insurance plans and/or tax-funded public health insurance programs such as Medicare and Medicaid. There are many statutes addressing health care fraud; among them are:

- 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. §§ 37293733).

Fraud Management—Activities that aid in the prevention, detection, and prosecution of fraud.

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 health care information, data, and knowledge for communication and decision making.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)—Public Law 104-191. The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addressed the security and privacy of health data.

Health Level Seven (HL7)—A data interchange protocol for health care 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 health care software vendor program HL7 interfaces for its products.

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 identity of each person who is a party to an EHR entry or transaction.

Improper Payment—In accordance with Office of Management and Budget (OMB) guidelines implementing the provisions of the Improper Payments Act of 2002, improper payments are those that should not have been made or were made in an incorrect amount.

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.

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 health care organizations. Medical informatics is as important to physicians and medical managers as the rules of financial accounting are to auditors.

Nonrepudiation—The EHR and/or interoperable NHIN 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—The public or private organization that is responsible for payment for health care expenses. Payers may be insurance companies or self-insured employers. Usually a third-party payer.

Personal Health Record (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 oneself or by a member of the person's family.

Prevention Functions—Those that occur prior to and during the documentation process in an EHR.

Prospective Functions—Those that occur after EHR documentation occurs but before a payment is made on any claim based on the EHR documentation.

Protected Health Information (PHI)—Individually identifiable health information transmitted or maintained in any form, which is related to the past, present, or future physical or mental health or condition of an individual.

Provider—A hospital or doctor who provides care. A health plan, managed care company, or insurance carrier is not a health care provider; these 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 a provider if the payer owns or manages providers, as with some staff model health management organizations.

Record Retention—Record retention requirements must be a minimum of 10 years. Presumably, patients would want their EHRs to be preserved forever because they represent patient medical history, except for transactional/billing records. Thus, law enforcement would need, at a minimum, to replicate current retention requirements for transactional records (i.e., 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 back-up (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 either redundant or back-up information.

Retrospective Functions—Those that occur after a claim has been paid.

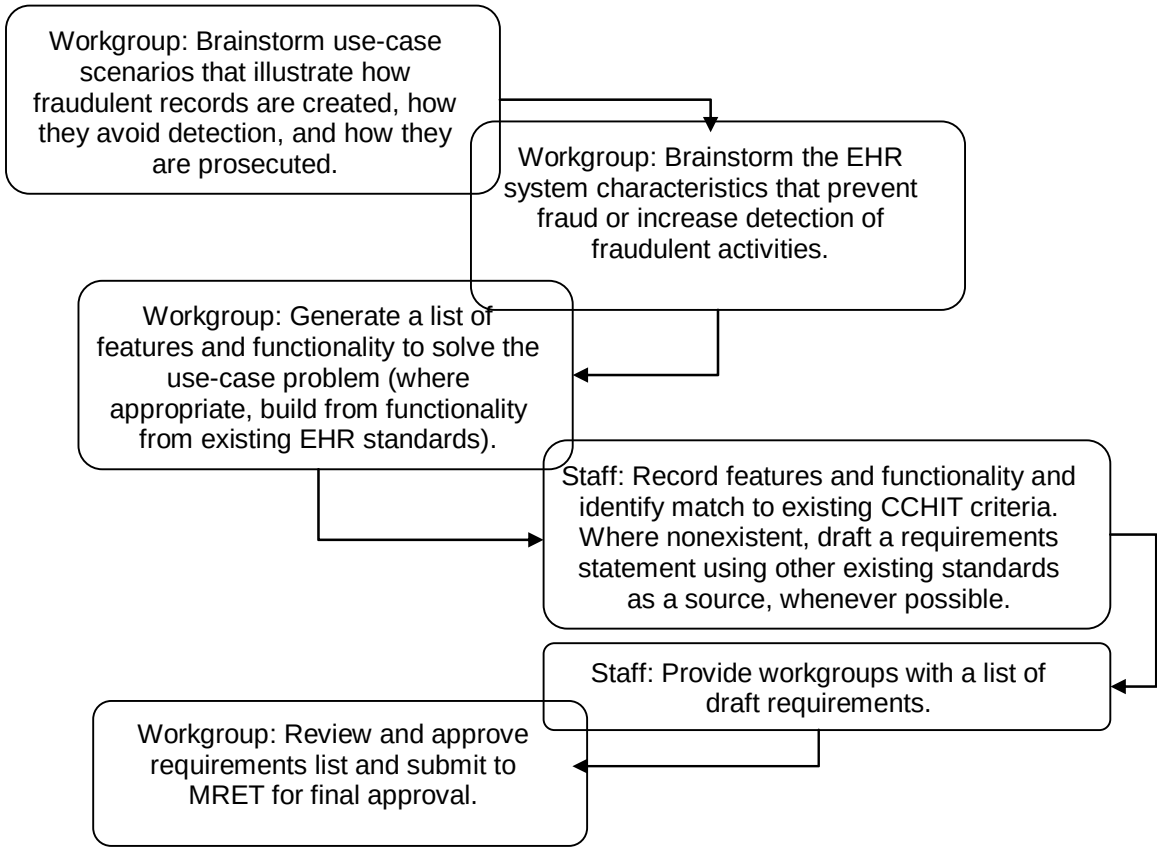
Storage and Security—EHRs and data transmitted and retained in an interoperable HIT system must be stored and be secure from access by unauthorized and unidentified persons or users. This applies to data stored in the United States and offshore. Records must be retained, unaltered, readable, and retrievable, 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—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.

Appendix D: Workgroup Process

As shown in ***Figure D-1***, each workgroup went through a process of first identifying a scenario of improper payment that fit under the focus charged to the group. All members were encouraged to submit use cases to serve as the platform for discussing what types of functional EHR requirements would aid in combating fraud in that particular case. The group was then asked to consider what characteristics an EHR system might require in order to combat the fraudulent activity. Using this information, members were asked to propose the functionalities that would support these characteristics, keeping a focus on current EHR standards whenever possible. The AHIMA project staff members quickly mapped these functionalities to existing CCHIT criteria. The final requirements were provided to the workgroup members for edits and other considerations before submitting the final list to the full MRET for another layer of review, discussion, and approval.

Figure D-1. Illustration of the MRET Workgroup Process



Appendix E: Tools Used for MRET and Public Validation Process

To facilitate these discussions, RTI provided a secure online project portal with a variety of tools intended to improve workflow for members of the MRET workgroups (***Figure E-1***). There were five main functionalities provided through the portal: Discussion Forums, Document Sharing, Shared Calendar, Group E-mail, and Contact Information. These functionalities provided some assistance to workgroup members in posing questions and ideas for consideration outside of the normal weekly meeting time. The portal also served as a repository for important background and administrative documents. Although use by members of the MRET workgroups varied, key members of the project team, such as the workgroup chairs, used the tools frequently to facilitate the large amount of work that needed to be done in only a few weeks.

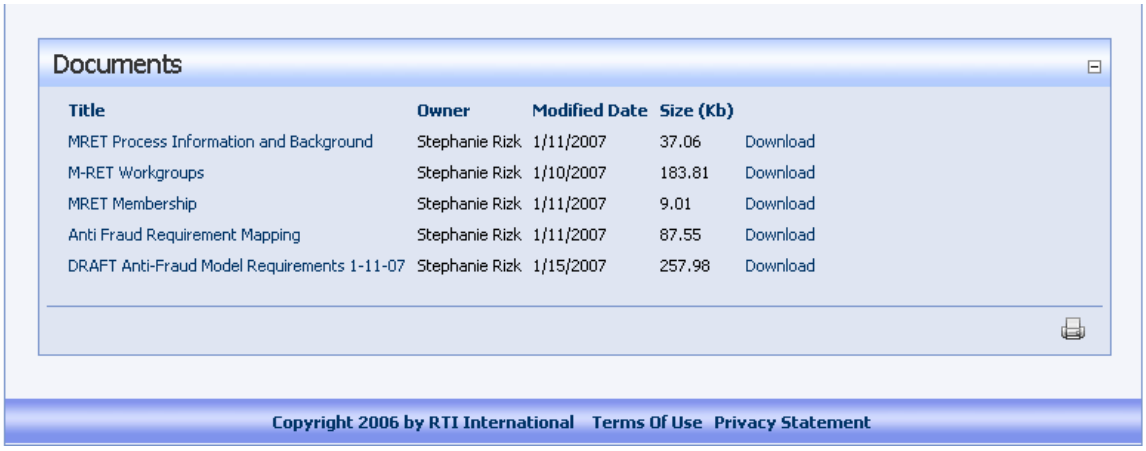
The online portal, set up and maintained by RTI staff, also allowed for the creation of public pages in addition to and separate from the private tools provided to facilitate MRET workgroup processes. This ability provided a natural platform for disseminating information to the general public and enabled quick and easy programming of a module that allowed registered users to submit secure and confidential feedback on each of the individual requirements.

Following a similar methodology to that used by CCHIT during their public comment process was expected to provide a sense of consistency within the stakeholder community. For this reason and for the purposes of accuracy in collecting the public comments and gauging the level of interest in the project, users were asked to register with the site before gaining access

Figure E-1. Main Public Page for Project Information

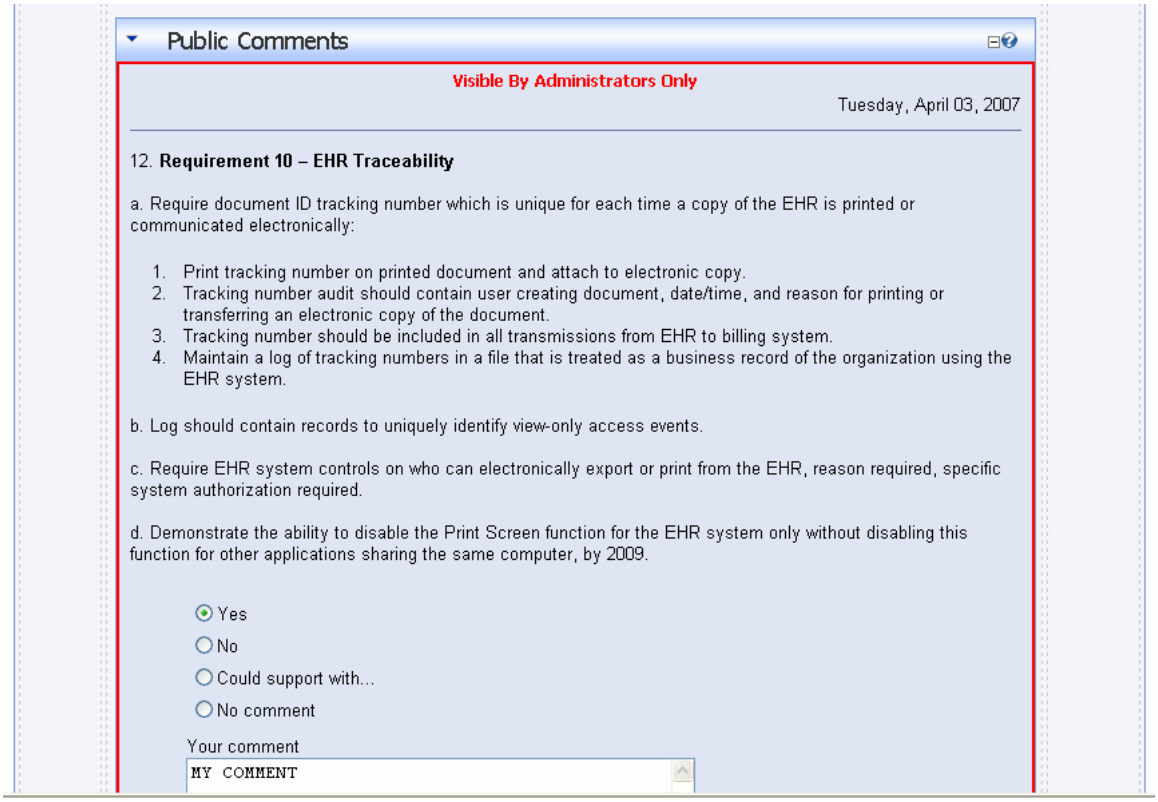
to the recommendations or the public comment module. The registration process was quick and easy, and once users had logged on to the site, they gained immediate access to the draft model requirements produced by the MRET and approved by ONC for public release (***Figure E-2***). In addition to the model-recommended functional requirements, this online process also allowed the project staff to include important context-setting documents, such as the MRET membership and workgroup processes, as well as a document that outlined mapping between the MRET recommendations and existing functional criteria accepted by leading groups such as HL7 and CCHIT.

Figure E-2. Documents Available upon Login



Once users had appropriate time to review and think about their response to the draft model requirements, they were instructed to access the Public Comment module. This module listed each requirement in succession and provided a comment box for users to provide their comments (***Figure E-3***).

Figure E-3. Example Screen of the Public Comment Module



Members of the core industry, government agencies, and the general public were encouraged to visit the site and provide feedback through a variety of methods, including general press releases, targeted e-mails, and personal/network connections.

Appendix F: Detailed Public Comment Analysis (Specific to Requirements)

As stated in Section 4.1 of the report, the public comments on the draft requirements fell into one of five categories:

1. Ability to Detect or Deter Fraud
2. Practicality of Implementation and Timeline Issues
3. Cost Issues
4. Burden and User Issues
5. Patient and Privacy Issues

Relevant excerpts from the comments are included below by requirement within each category. Where patterns emerged among a certain type of respondent (e.g., physician, HIT vendor), they are also presented in the relevant category.

F.1 Category #1: Ability to Detect or Deter Fraud

F.1.1 Comments on Requirement Overall

- One reviewer stated, "Post-processing is all that is required to identify the most likely fraud candidates." While another reviewer stated, "The solution to fraud is better data mining of claims and health records by experienced auditors and a smart computer system that detects data anomalies."

F.1.2 Requirement-Specific Comments

- Audit Functions and Features: Some reviewers expressed concern about viewing and printing records. One reviewer cautioned that "if the record has been 'viewed' assume that it could easily be printed, copied, or photographed. By the time it has been printed, it has already been thoroughly compromised." Another reviewer commented that "records should not be printable or transferable."

- User Access Authorization: One health care purchaser/payer noted that "this would greatly reduce the amount of fraudulent activity and attempted breaches of information."

- Documentation Process Issues: One reviewer noted that the rationale for the Documentation Process Issues requirement was weak and asked, "How does direct data entry with mouse versus keyboard indicate fraud?" Another noted it is "reasonable to ask for a record on whether the note was completed through a voice recognition system such as dragon or whether it was created through a template, or dictated," however the reviewer did not see how "going further than that adds significant value." Yet another reviewer commented that "having the ability to audit the various ways to enter notes in an EHR system would provide good anti-fraud capabilities since many EHR systems allow users to dictate or copy and paste notes into the system. Auditing these events would catch suspicious activity."

- Copying Notes: A reviewer was uncertain whether the requirement could detect fraud and stated, "While this requirement gives the impression that fraud exists because the findings are the same, the reality is it is common for patients to have the same findings as a prior visit or a recent patient with a similar problem. The vast majority of the time this would simply clutter the chart and the number of positives would be too great to be useful at combating fraud."

- E&M Coding: A reviewer commented that "if anything, this might encourage fraud as it flags documentation as being inadequate for the billing which the physician believes is warranted."

- Proxy Authorship: Two reviewers were confident that this requirement would be effective. One noted it would be "beneficial since many providers have assistants." The other mentioned that the situation "comes up all the time when interns' entries and orders need to be countersigned." However, others questioned its usefulness, such as one who noted, "This will only affect legitimate providers who do not share their authorization codes/tokens. Fraudulent billers will simply allow assistants to log in as the biller."

- Record Modification after Signature: One reviewer felt it would help accountability and stated, "we fully support retention of original documents and any amendments after signature event for accountability purposes."

- Data Aggregation and Access at the Patient Level: A reviewer felt access to even more information than the recommendation proposed was critical, stating, "Where fraud is suspected, very often being able to review the entire 'episode of care' is critical. As a result, in some instances medical records for service dates that fall outside the time period of potentially fraudulent services are critical to an audit or review."

- EHR Traceability: A reviewer commented it was "fine for privacy and security," but the respondent did not see how the requirement was helpful in fraud detection.

- Patient Involvement in Anti-Fraud: A reviewer was uncertain how this requirement would aid in detecting fraud; however, another noted that "having the ability for patients to view their own record is a good way to prevent fraud and reduce errors."

- Integrity of EHR Transmission: A reviewer felt that "this might be a billing or data interchange (RHIO [regional health information organization]) issue, but it is not an anti-fraud issue."

- Structured and Coded Data: A reviewer supported this recommendation, noting "The use of codes in an EHR system will reduce fraud through the use of analytics and pattern detection."

- Accurate Linkage of Claims to Clinical Records: Support was supplied by two reviewers. The first noted, "Integrity and retention of audit files with full accountability of EHR encounters is paramount," while the second stated, "This is a fundamental feature to ensure the proper clinical record is referencing the claim."

F.2 Category #2: Practicality of Implementation and Timeline Issues

F.2.1 Requirement-Specific Comments

- Audit Functions and Features: One reviewer noted support if "vendors were given lead time," while two others commented that "the data to be collected is vastly too much to be practical" and the requirement was "not realistic." Another reviewer felt there was a "need to reduce the minimum data set." More specifically, another reviewer cautioned "date/time/user stamp at the data element level would create a significant burden for application developers and require substantial programming," while another voiced concern "about the requirement to stamp each clinical entry at the data element level."

- Provider Identification: A reviewer cautioned that this requirement should only be put into place "when the NPI is fully supported by the industry." Other reviewers had concerns regarding the logistics having to do with multiple NPIs, how to handle those without NPIs, and how to define NPIs at the organization level. Finally, one reviewer expressed concern because the NPI has "limited international identification capability."

- User Access Authorization: One reviewer stated, "Biometrics, tokens, and PKI are well established technology. What reasons are given to push this timeline for adoption out to 2010 nor 2012?" Another reviewer agreed and "strongly recommended" the dates be moved forward. However, other reviewers felt it was "not likely" that implementation could occur in 3 years. One reviewer suggested a more practical solution would be to recommend systems-support existing guidelines from the National Institute of Standards and Technology or the Office of Management and Budget rather than determining specific technology measures.

- Documentation Process Issues: Some reviewers did not support this requirement, commenting that "this approach is neither effective nor valid" and "it is beyond the scope of most applications today to track this detail." Another reviewer questioned the relevance and noted that the data to be captured included "nice to have fields that might lead to something useful, some day."

- Copying Notes: It was suggested that this would be impractical because all of their "tools are web-based and copying is done via the native capabilities of the operating system, which cannot be controlled by our applications."

- E&M Coding: A reviewer cautioned that "systems should be reviewed by qualified e/m [evaluation and management] compliance experts," and another noted that "if EHR-S were not able to promote e&m [evaluation and management] documentation, then major utility for providers is lost." However, another reviewer felt that "the EMR should never be used by a facilitator of 'up-coding.'"

- Data Aggregation and Access at the Patient Level: A reviewer noted that the requirement is "highly impractical due to the divergent information needs of the various payers."

- EHR Traceability: Reviewers expressed concerns regarding feasibility. One reviewer noted that "disabling the print screen is only of minimal use, since twain-compliant screen capture software is readily available for all thick-client platforms such as PC's." It was also noted that "EHRs applications may be unable to control either the user invoked print or the actual content printed," and another reviewer recommended "defining strictly who can electronically export or print from the EHR with full documentation of reason and no automated printing function."

- Patient Involvement in Anti-Fraud: One reviewer noted that "this standard will add an enormous amount of time to the HIM [health information management] department's functions," and another questioned "how do you [ensure] patient entered comments are in the correct place & how will anyone know to take any action?"

- Patient Identification: Some reviewers voiced concerns about the use of the proposed technology and the timeline. One reviewer felt that the "downside is the amount of storage required." Another noted that "issues related to potential theft of biometric identifiers should be thoroughly researched and resolved before requiring widespread adoption." Also, one cautioned that "many patients will not be comfortable with electronic capture of their identity tokens, and this may interfere with their decisions about accessing care." Other comments were related to the timeline, with one reviewer noting that implementation was suggested in "too soon a time" and another stating uncertainty about whether the date supplied was "realistic."

- Structured and Coded Data: One reviewer felt this was "too futuristic." Another agreed and commented, "I do not believe the technology is mature enough to support machine conversion of non-structured input into structured data." Another was "not sure this reqt [requirement] is practically achievable, especially given different coding systems and updates." Lastly, another commented that "conversion of non-structured text is too machine intensive today."

- Accurate Linkage of Claims to Clinical Records: Reviewers commented on the timeline and feasibility. One noted that payer systems do not support such functionality and it is unlikely they will in the next 10 years." Another commented that "both the billing and the clinical records systems will have to be compatible and currently there are so many systems out there that do not speak to one another that this will have to have year(s) of testing."

F.3 Category #3: Cost Issues

F.3.1 Requirement-Specific Comments

- Audit Functions and Features: Some expressed concern that significant expense would be incurred for data storage, software, development, and maintenance. One reviewer commented that the requirement might be acceptable "if the government or possibly payers want to give EHRs away for free." Another respondent was concerned that some "provider organizations" are small and cannot afford expensive systems.

- Provider Identification: One reviewer felt that there needed to be a "better understanding of impact on hospital operations and costs associated with implementing."

- User Access Authorization: Health care purchasers/payers were concerned with funding, "especially for the biometrics ability." One reviewer cautioned that there "needs to be a true understanding of costs involved before creating such standards."

- Documentation Process Issues: The comment was again made that requirements such as those listed require a formal cost-benefit evaluation before they are required. (Health care purchasers/payers had similar concerns about Requirement 5: Copying Notes). One reviewer felt that the requirement was "likely to alienate and scare away potential adopters, both from a price prospective, as well as a fear of unfair prosecution." Another felt the requirement was fine as long as it would not be "overly costly to hospitals."

- E&M Coding: One reviewer felt that the requirement was "unreasonable for a small, inexpensive EHR, especially one that focuses in behavioral health." Other comments suggested that some requirements might be too costly for some small-scale systems.

- Data Aggregation and Access at the Patient Level: A reviewer felt that the requirement "would create enormous problems for the small and medium size medical practice, raising costs of EHR use."

- Patient Identification: One reviewer asked, "Who will pay for the hardware?" Another was concerned about the cost of biometrics, asking, "How much money must be spent for this to happen?"

F.4 Category #4: Burden and User Issues

F.4.1 Comments on Requirement Overall

- One reviewer commented, "Fraud is not prevented by forcing computer systems to be so complex, burdensome and expensive their use is actually discouraged." Another noted that the requirements were intended to "establish complex policing actions that increase the complexity of these systems and create greater hurdles for physicians in providing high quality, compliant and efficient care."

F.4.2 Requirement-Specific Comments

- Provider Identification: A reviewer commented on the need to gain a "better understanding of the impact on hospital operations and costs associated with implementing" the requirements.

- User Access Authorization: One respondent felt that "it should be up to the provider to decide which, if any, to use, in accordance with existing laws and regulations." In addition, another reviewer recommended that the requirement "permit entities to take advantage of the latest technological solution and industry accepted methods." Another respondent was concerned that the requirement "puts an onerous burden on small provider organizations."

- Documentation Process Issues: A reviewer noted the need for a "practical understanding of costs." Another reviewer mentioned it was "unnecessarily burdensome" and could "slow down the entry of data," while another felt that it could "adversely affect productivity."

- Copying Notes: A respondent felt that this requirement "fails to correct the underlying compliance issue but rather sets up a complex monitoring system which will further interfere with patient care and alienate physicians."

- E&M Coding: Two HIT vendors supplied comments. The first mentioned the need to "strike a balance between fraud prevention and user/workflow productivity," while the second added that "EHRs are not primarily anti-fraud devices."

- Proxy Authorship: One reviewer could only support the recommendation if "it could be shown that the existence of such an audit trail would not disrupt or distort patient care workflows." However, another reviewer commented that this information was "typically required by clinicians anyway."

- EHR Traceability: A reviewer commented that traceability is "an overburdensome task for the user."

- Patient Involvement in Anti-Fraud: A reviewer felt that this "would create a lot of time wasted from the providers' perspective."

- Patient Identification: A reviewer summarized that "the standard should accommodate a cost/benefit analysis by the user based on risk, industry-wide accepted solutions and individual system capabilities."

F.5 Category #5: Patient and Privacy Issues

F.5.1 Requirement-Specific Comments

- Audit Functions and Features: One reviewer was concerned with physician privacy, noting the requirements "are intrusive and will deter use of the EHR."

- Copying Notes: A reviewer felt it was "important for privacy as well as integrity of patient data" and another agreed, noting it was "very important to integrity of the record."

- Data Aggregation and Access at the Patient Level: With regard to patient and privacy issues, two health care payers/purchasers noted that "payers should not have [an]

unfettered right to access [a] hospital data base" and "insurance payers should not have electronic access to records." Others noted that there was not "justification for a payer to have such relatively unbridled access to an EHR" and voiced concerns about whether this was "a violation of privacy" and whether "patients or patient advocacy groups would accept this." The remaining comments for Requirement 9 were from reviewers who either provided support contingent on their comment or supported the requirement and requested consideration for the information provided. All voiced similar concerns. specifically noting the need for restricted access and maintenance of "physician-patient confidentiality" to ensure patients' rights and privacy are protected along with the need to "[ensure] compliance with HIPAA."

- Patient Involvement in Anti-Fraud: Two physicians agreed that "all EMRs should allow the patient to view his full history" and "patients commenting in the EHR should be carefully allowed & occur in reasonable ways, at reasonable times." Furthermore, health care purchasers/payers noted that "only the patient and doctor should have access to records electronically" and there is a need for "additional capability to prohibit physicians from any further 'use' of patient information/record when requested by patient." One reviewer commented on the "need to harmonize with the HIPAA requirements," while another noted that "we feel that a specific requirement to allow a patient the ability to 'comment in the her' totally ignores the information safeguards put into play by the HIPAA requirements for requesting amendment to the patient record." A concerned reviewer cautioned that "although this is most helpful, in a behavioral/mental health or substance abuse setting, providing the patient with ability to view clinical information may cause undue harm and place a patient or other at risk," while another noted that access has to be made "equally available to all patients regardless of personal limitations, such as inability to use a computer."

- Patient Identification: One reviewer cautioned that "there are pretty strong privacy concerns about these approaches. Consider using some 'secret' questions and answers." Two additional reviewers noted that they could support this requirement if "consent of the patient" was obtained. Another reviewer noted that "fraud prevention methods should not infringe upon individual rights."

- Integrity of EHR Transmission: One reviewer felt "this is very important to patient confidence in the EHR."

Appendix G: Mapping Requirements to CCHIT/HL7 Criteria

Table G-1. Audit Functions and Features

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
1.1 Require a standardized audit log that supports both security risk management and fraud management. 1.1.1 Date/time/user stamp for each clinical entry at data element level or some other suitable mechanism to allow assessment of the number of user operations used to create an encounter note or encounter note update. 1.1.2 Date/time/user stamp of each access to the EHR. 1.1.3 Date/time/user stamp of "signature event" (whether proactive or auto default) for encounter or progress notes. 1.1.4 Date/time of release of encounter or progress note for administrative/billing process or, alternatively, date/time billing transaction was created based on encounter or progress note. 1.1.5 Minimum data to be captured in the audit log includes the following:	2008	A comprehensive fraud management program, which encompasses the prevention, detection, and prosecution of health care fraud, requires efforts at multiple levels, most of which occur outside of the EHR. For fraud that involves the creation of fraudulent claims based on clinical services provided to patients, the EHR in all of its aspects is central to fraud management in important ways. For prevention, the mere fact of knowing that information is being collected on the process and content of clinical documentation that could be used to detect fraudulent behavior in itself serves as a deterrent to that behavior. Audit reports provide the tools to self-monitor and apply preventive strategies before detection or prosecution. The audit log provides the who, what, when, where, why, and how in this cycle. This log is central to prevention, detection, and prosecution of health care fraud.		Security Audit: The system shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include: start/stop, user login/logout, session time-out, account lockout, patient record created/viewed/updated/deleted, scheduling, query, order, node-authentication failure, signature created/validated, PHI export (e.g., print), PHI import, and security administration events. Note: The system is only responsible for auditing security events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security events that it does not mediate.	The system shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include: start/stop, user login/logout, session time-out, account lockout, patient record created/viewed/updated/deleted, The logical location from which information was accessed if known (e.g., PC address, UMS socket address, Internet address), Scheduling, Query, Order, Node-authentication failure, Signature created/validated, PHI export/print, User-entered reason for export/print, PHI import, and security administration events. Note: The system is only responsible for auditing security and clinical record events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security and clinical record events that it does not mediate.		

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
1.1.5.1 Access type (i.e., creating, editing, viewing, printing, or electronically transferring all or any part of the patient record) 1.1.5.2 User ID, including National Provider Identifier (NPI) number if available, of person accessing the record 1.1.5.3 Location or logical address from which the information was accessed 1.1.5.4 Date and time that the information was accessed using NTP/SNTP synchronized time 1.1.5.5 For printing or transferring electronically all or parts of a record that is initiated by a user, reason for transaction entered by user							

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
			S6 Partial Match 1.1.1, 1.1.2, 1.1.5.2, 1.1.5.4	Security Audit: The system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the information system (e.g., software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g., user identity); and (5) the outcome (success or failure) of the event.	The system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the information system (e.g., software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g., user identity); (5) the outcome (success or failure) of the event, (6) the date and time of release of clinical documentation for administrative/billing purposes or date/time billing transaction was created based on the clinical documentation encounter or progress note.		
			S8.1 Partial Match 1.1.5.4	Security Audit: The system shall be able to provide time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.	The system shall be able to provide time synchronization using NTP/SNTP, and use this synchronized time in all security records and clinical record event logs of time.		
			No Match 1.1.4 and 1.1.5.3		See proposed language above: 1.1.4: Date and time release of documentation for billing (see 5.3 above) 1.1.5.3: Location or logical address from which information was accessed (see 5.2 above).		

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
1.1.6 The audit log will be operational whenever the system is available for updates or viewing of the clinical record. There may be exceptional circumstances for technical or other reasons when this cannot occur: 1.1.6.1 If the system supports a user command to disable or enable the audit log, such command shall be limited to roles associated with users that administer the system. 1.1.6.2 All user commands that enable or disable the audit log shall be recorded in the audit log as auditable events. 1.1.6.3 If the system is accepting updates at a time when the audit log is impaired or disabled, a notification of the occurrence of this state will be made available to the system administrator.		Much of fraud detection revolves around analyzing patterns of information available in claims and other databases that raise the suspicion of fraudulent behavior for further investigation. The more detailed information available to these pattern-detection systems, the greater the ability to differentiate legitimate from fraudulent behavior. When a suspicious pattern, which would be pre-determined based upon historical analysis of similar data, is detected, the ability to reconstruct further detail regarding the who, what, when, where, why, and how of clinical documentation provides the tools for investigation. Furthermore, when fraud is detected, these same tools can be used for prosecution.	No Match 1.1.6.1		S11 The system shall allow an authorized administrator to set the inclusion or exclusion of audited events based on organizational policy and operating requirements/limits, however, the minimum auditable events in S5.2 and S5.3 may not be excluded regardless of organizational policy. NEW S11.1: The system shall log audit information in S5.2 and S5.3 when in operation except for unavoidable technical circumstances (e.g., software problems, technical failure, full storage capacity, etc.) (Propose for inclusion on roadmap in 2009)		

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
1.1.6.4 The audit log shall support a means of unequivocally determining if it contains gaps when users updated the record while the audit log was not being recorded, even if the audit log was not recorded for a reason other than explicit disablement by a user. Such determination shall be evident solely by examining the audit log.		The continuing iterative process above enables not only the creation of prospective screening tools to prevent payment of fraudulent claims, but allows evolution of those tools as the perpetrators of fraud become increasingly sophisticated in their methods. Some of these preventive measures can be built into the EHRs themselves to prevent the creation of fraudulent documentation.					
			No Match 1.1.6.2, 1.1.6.3, 1.1.6.4		NEW S11.2 The system shall audit commands to disable or enable other audit logs. NEW S11.3 The system shall notify the system administrator if the system is accepting updates when the audit log is impaired or disabled. NEW S11.4 The system shall provide an audit report that show gaps when users were updating the record/PHI when audit functionality was disabled for any reason (e.g., disablement, technical, etc.).		

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
1.1.7 Deletions or alteration of the contents of the audit log will not be allowed by users.			2007 S9 Match	Security Audit: The system shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. The system shall protect the stored audit records from unauthorized deletion. The system shall prevent modifications to the audit record.			
1.1.8 System must support a user-friendly output version of the audit log for transmission, printing, or export, which shows all details of events described in 1.1.1–1.1.5 above.			S7 Match with suggestion	The system shall provide authorized administrators with the capability to read all audit information from the audit recordsin one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format and correlate	The system shall provide authorized administrators with the capability to read all audit information from the audit recordsin one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format and correlate records based on time (e.g., UTC synchronization). 3) The system shall be able to provide a user-friendly		

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
1.2 Audit Support Function: Require documentation of the audit support functionality in the vendor provided user guides and other support documentation, including how to identify and retrospectively reconstruct all data elements in the audit log including date, time and method of entry.	2008	We are cognizant of the issues surrounding the requirements for audit functionality and recommend alternatives to the following questions: 1. Will the process of creating and maintaining the audit log impair the performance of the EHR system? If this is the case, we do not recommend its implementation in all aspects (1a-1c), but rather a phase-in of as much as possible over time, without interfering with performance. Some vendors are able to do all of this now, while others can do little. It will be the task of CCHIT to determine the appropriate timing for specific implementation certification criteria. 2. Will access to this level of detail by authorized entities involved in fraud management pose a problem for privacy of patients or violate physicians' rights? The risk exists that such access, if used inappropriately, could pose a problem.	S23 Partial match	records based on time (e.g., UTC synchronization).	audit log for specified information/views/functions for all items in S5.2/S5.3. The log shall be available for transmission, printing or export when needed or requested. The system shall include documentation that covers: Guidelines for proper configuration of the EHR security controls (~~e.g.,~~ including users, roles management, password management, audit logs and how to identify and retrospectively reconstruct data elements in the audit log) necessary for proper secure and reliable operations of the system.		

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
		Therefore, we recommend that this access be strictly limited according to all levels of law, policy, and local practice. 3. Will this add too much cost to EHRs? It will add some cost, as do most modifications to software. However, with appropriate design, we believe that the added costs can be minimized to levels that are cost-effective for EHRs. Stakeholders should also consider the trade-off gains from recovering dollars from improper payments compared to losses that would continue to be incurred if the recommended functionality is not implemented. 4. Is this appropriate for all clinical settings? We recommend that it first be applied in the ambulatory area and then modifications be made, as necessary, as requirements are developed for other settings.					

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
1.3 The system shall have the capacity to allow authorized entities to read only access according to agreed upon uses and only as a part of an identified audit subject to appropriate authentication, authorization, and access control procedures. Such access shall also be subject to appropriate release of information protocols, local audit policies, minimum necessary criteria, and other contractual arrangements and, laws, and:	2008		S7 Partial Match 1.3, 1.3.2	Security Audit: The system shall provide authorized administrators with the capability to read all audit information from the audit recordsin one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format and correlate records based on time (e.g., UTC synchronization).	See S7 above for added text		
1.3.1 Require “auditor” be a supported class of user			S1 Match with suggestion	Security Access Control: The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g., system administrator, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.	The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups including external auditor as a supported class of users, or processes acting on behalf of users, for the performance of specified tasks.		

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
1.3.2 Limit access to pertinent functions and views only for portions of audit logs covered by the audit.			S7 Partial Match Above	See above	See S7 above for added text		
1.3.3 Access remains controlled by the facility and the same authentication and audit supports would apply.			S3 Match with suggestion	Security Access Control: The system must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role based (users are grouped and access rights assigned to these groups); or 3) context based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation location, emergency-mode, etc.)	The system much be able to associate permissions, including permissions for a remote access user, with a user (e.g., system administrator, Clerical, Nurse, Doctor, etc.) using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role based (users are grouped and access rights assigned to these groups); or 3) context based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation location, emergency-mode, etc.)		
1.3.4 Remote access may be offered if agreed to by the clinical data organization subject to the aforementioned protocols and suitable authentication			S12 Partial Match	Security Authentication: The system shall authenticate the user before any access to protected resources (e.g., PHI) is allowed including when not connected to a network e.g., mobile devices.	The system shall authenticate the user (including a remote access user) before any access to protected resources (e.g., PHI) is allowed including when not connected to a network e.g., mobile devices.		

(continued)

Table G-1. Audit Functions and Features (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function / Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function / Criteria[b]
1.4 Data and Document Retention, Disposal and Archiving: Retain all EHR system data and clinical documents (including audit logs) for the time periods designated by the EHR system owner's policies or legal requirements. Audit logs should be retained as long as clinical records. Provide the ability to destroy, deactivate, or archive EHR data/records in a systematic way according to the EHR system owner's policies and after legally-prescribed retention periods.	2008		F252 Match with suggestion	Retention, Availability & Destruction: The system shall retain data until otherwise purged, deleted, archived or otherwise deliberately removed.	The system shall retain data (including audit records) until otherwise purged, deleted, archived or otherwise deliberately removed per EHR-S owner's policy after legally-prescribed retention period.		

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-2. Mapping Requirement 2: Provider Identification to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/Criteria[b]
2. EHR-S must support the use of the NPI* in the EHR audit log to identify the individual provider, or, in situations when an NPI is not available for an individual, a single unique internal provider identifier is assigned.	2008	A commonly known fraud scheme is for fraud perpetrators to steal provider identifiers and use them to submit false claims. Use of the NPI in EHRs as well as claims will significantly reduce fraud losses. The NPI is required to be on electronic claims beginning in May 2007 for large health care providers and May 2008 for small health care providers. Use of the NPI would also enable payers to remit claims payments only to registered providers at their registered locations further reducing the motivation for Provider ID theft.Further, in order to investigate health care fraud, it is necessary to have either the NPI or a unique internal provider ID attached to all transactions in the EHR for inclusion in all EHR transaction logs. This requirement documents the author of an entry in an EHR.	F211 Partial Match (Collect NPI)	Provider Demographics: The system shall maintain a directory which contains identifiers required for licensed clinicians to support the practice of medicine including at a minimum state medical license, DEA, NPI and UPIN number.	Provider Demographics: The system shall maintain a directory which contains identifiers required for licensed clinicians to support the practice of medicine including at a minimum state medical license, DEA, NPI and UPIN number. (Note: The NPI is the preferred identifier. The system shall assign a unique identifier if the user does not have an NPI.)		

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-3. Mapping Requirement 3: User Access Authentication to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/Criteria[b]
3.1 Demonstrate the ability to support user ID/strong password in 2008.	2008	Fraud prevention is enabled by requiring user authentication to the EHR. The health care entity bears responsibility for assuring that all individuals authorized to access the EHR have the requisite credentials for the services they provide. Validation of the process of credentialing in the EHR will allow matching of the provider profile to the type of services billed.	S13 Match	Security Authentication: When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.			
3.2 Demonstrate the ability to evolve the level of user authentication in the future as industry standards require.	2009	NCVHS and CCHIT both have released roadmap documents that speak to proposed authentication technology requirements. Both entities have expressed a requirement for userID/strong password by 2008. In the case of the CCHIT roadmap, these include PKI and enhanced authentication as goals for 2009 and beyond. These recommendations endorse the roadmaps and encourage the continual technological growth of authentication practices in EHR-S.	2007 S31 Match	Security Authentication: The system shall support two-factor authentication in alignment with NIST 800-63 Level 3 Authentication. Note: The standards in this area are still evolving.			

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-4. Mapping Requirement 4: Documentation Process Issues to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
4. System will provide the capability to produce a business version of a clinical document which indicates	2008	EHRs provide various tools that enable a provider to be more efficient of his/her time when documenting an encounter. These include the use of defaults, templates, copying and other tools. These are legitimate benefits of using an automated system; however they could be subject to fraud or abuse. The intent is not to audit or monitor encounter notes, as this would have limited impact on proactive fraud monitoring. The use of copy/paste, default forward and/or import functions is left to the discretion of the user of the EHR system. However, having an audit version of the EHR which indicates which of these tools were used could enable retroactive detection of patterns of abuse or fraud.	No Match		New**:** The system shall produce a business version of a clinical document that includes date, time and user stamp.	No Match	
4.1 Date/time/user stamp for each entry					New: The system shall produce a business version of a clinical document that specifies the method of creation (1) Direct entry via integrated hardware keyboard or mouse (2) Speech recognition (3) Automated, machine-entered default information (4) Pre-created documentation via form or template (5) Copy/import of an object including date/time user stamp of original author (6) Copy forward previous note contents including date/time user stamp of original author (7) Dictation/ Transcription (8) Import from an external system		
4.2 The methods used in the creation of the entry including but not limited to			No Match				
4.2.1 Direct entry via integrated hardware keyboard or mouse							
4.2.2 Speech recognition							
4.2.3 Automated, machine-entered default information							
4.2.4 Precreated documentation via form or template							
4.2.5 Copy/import of an object including date/time user stamp of original author							
4.2.6 Copy forward previous note contents, including date/time user stamp of original author							
4.2.7 Dictation/transcription							
4.2.8 Import from an external system.							
4.3 If a copy of the encounter note is required or desired to accompany a claim, provide the ability to submit the business version.					New: The system shall provide the ability to produce for business version of a clinical document for disclosure purposes when requested or required.		

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-5. Mapping Requirement 5: Evaluation and Management (E&M) Coding to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
5.1 The system shall be capable of prompting for omitted necessary administrative data or codes. This could include the capability to prompt a clinician if the selected E&M code is not consistent with the documentation in the encounter note.	2008	This is new wording for CCHIT requirement #237 of the Ambulatory functional requirements which states, "The system shall prompt for data required to determine appropriate administrative (evaluation and management) codes if such data is not present in encounter data." It is appropriate for EHRs to calculate an Evaluation and Management (E&M) code from the encounter data which has been entered and to indicate the basis for that calculation. However, it is not appropriate to suggest to the provider that certain additional data, if entered, would increase the level of the E&M code. The wording of the current CCHIT requirement, although unintended, could be interpreted to suggest the latter.	F234, F236 Match	Rules-driven Financial & Administrative Coding Assistance: F234) The system shall provide a list of financial and administrative codes. F236) The system shall provide assistance in selecting appropriate billing codes based on codified clinical information in the encounter.			
5.2 Prompts that are driven by E&M administrative processes will not explicitly or implicitly direct a user to add documentation. This does not apply to prompts for additional documentation for E&M levels already achieved, for medical necessity, or for quality guidelines/clinical decision support.	2008		F235 Partial Match	Rules-driven Financial & Administrative Coding Assistance: The system shall provide the ability to select an appropriate CPT E&M code based on data found in a clinical encounter.	The system shall provide the ability to select an appropriate CPT E&M code based on data found in a clinical encounter and not implicitly or explicitly prompt the user to add documentation specifically aimed at increasing the E&M level.		

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-6. Mapping Requirement 6: Proxy Authorship to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
6.1 Retain date/time/user stamp of original data entry person when data entered "on behalf" of another author.	2008	A provider's staff can obtain information from a patient and put the information into the clinical record, or the provider can obtain the information from a patient and have the staff record the information on his/her behalf. It is important to be able to distinguish which, if either, of these mechanisms was utilized.	F58 Partial Match	The system shall record the identity of the user finalizing each note and the date and time of finalization.	See HL7 standard DC.1.8.5 Manage Clinical Documents and Notes to further address the intent of this requirement: The system shall provide the ability to record, and display the identity of all users entering data, contributing to or finalizing a document or note, including the date and time of entry (see appropriate criteria in IN.2.2).	DC.1.8.5 Partial Match (to both 6a and 6b)	Manage Clinical Documents and Notes: The system shall provide the ability to attribute record and display the identity of all users contributing to or finalizing a document or note, including the date and time of entry (see appropriate criteria in IN.2.2).
6.2 If an assistant is used to enter data that will subsequently be signed by a provider, retain the date/time/use stamp of the data entry person as well as the provider.	2008		F58 Partial Match Same as above	Same as above	Same as above		

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-7. Mapping Requirement 7: Record Modification after Signature to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
7. Require amended note with retention of original after "signature event" (including automatic "closing" of record).	2008	There needs to be some point in the process of documenting an encounter when that documentation cannot be altered without retaining an audit trail of the original entry. That is typically at the time when the provider "signs" a note electronically or when a practice automatically "closes" an encounter at some specified time period after the encounter. Retaining an audit trail of changes after this event prevents fraudulent alteration of the record at a later time.	F60 Partial Match	Manage Clinical Documents and Notes: The system shall provide the ability to addend and/or correct notes that have been finalized.	Manage Clinical Documents and Notes: The system shall provide the ability to addend and/or correct notes that have been finalized whether by the user or auto-finalized by the system. The system shall retain the original content of the note before an addendum or correction was made.		

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-8. Mapping Requirement 8: Auditor Access to Patient Record to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
8. The system shall have the capacity to allow authorized entities read-only access to the EHR according to agreed upon uses and only as part of an identified audit subject to appropriate authentication, authorization, and access control functionality. Such access controls shall also support the applicable release of information protocols, local audit policies, minimum necessary criteria, and other contractual arrangements and laws, and	2008	Detection of a fraudulent claim is often difficult when a payer has access only to EHR information for a single encounter. Reviewing information over an entire episode of care for a single patient allows greater ability to detect fraud. Access should be limited and subject to compliance with HIPAA, other federal and state laws, and applicable contractual agreements between the provider organization and payer.	Partial Match See 1.3 above				
8.1 Require "auditor" be a supported class of user.			Match See 1.3.1 above				
8.2 Limit access to pertinent functions and views only for patient records covered by the audit..			Partial Match See 1.3.2 above				
8.3 Access remains controlled by the facility and the same authentication and audit supports would apply..			Match See 1.3.3 above				
8.4 Remote access may be offered if agreed to by the organization subject to the aforementioned protocols and suitable authentication.			Partial Match See 1.3.4 above				
8.5 Demonstrate the ability to provide a paper copy of such information in the event access to the EHR is not possible.			F224 Match	Health Record Output: The system shall provide the ability to define one or more reports as the formal health record for disclosure purposes.			

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-9. Mapping Requirement 9: EHR Traceability to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
9.1 Demonstrate the ability to generate and embed a document ID tracking number to patient chart outputs or exports, unique for each instance when a patient chart output/document is printed, electronically communicated, or otherwise exported from the EHR.	2008	It is typically easier and more credible to create a fraudulent claim by utilizing real patient record information than attempting to fabricate this information de novo. Preventing the unauthorized transfer, printing, and viewing of patient records reduces the ability to obtain such information. Function 9 also assumes that the EHR system's ability to track documentation events will support the reconstruction of how the export was created and thereby allow reconstruction and audit of its contents when necessary.	No Match		New: The system shall have the ability to assign a document ID tracking number for each instance a document or record is printed or exported.		
9.1.1 Display tracking number on printed document (regardless of the document format including, but not be limited to, .doc, .pdf, and attach to electronic copy.	2008		No Match	Note: CCHIT comments to the MRET state that standards are in early development and that it is doable using CDA Release 2. Each doc inherently has a globally unique object identifier.	New: F224.1 Health Record Output - Tracking Number: The system shall provide the ability to define one or more reports as the formal health record for disclosure purposes and display the print tracking number for each instance the document is printed or exported (including export to a separate billing system).		
9.1.2 Tracking number audit record should contain user creating document, date/time, and the reason for printing or transferring an electronic copy of the document (if available)	2008		F247 Partial Match (Also relates to S5.3)	Enforcement of Confidentiality: The system shall audit the date/time and user of each instance when a patient chart is printed by the system.	The system shall audit the date/time and user of each instance when a patient chart is printed and record user-entered reason for printing or transferring an electronic copy of a document or record if available.		
9.1.3 Tracking number function requirement also applies to transfers of information from the EHR system to a billing system where these are separate or otherwise independently functioning systems	2008		No Match		See above New F224.1 - printed or exported		

(continued)

Table G-9. Mapping Requirement 9: EHR Traceability to CCHIT/HL7 Criteria (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
9.1.4 Maintain an audit log of tracking numbers in a file that is treated as a business record of the organization.	2008		No Match		New: The system shall be able to generate an audit record/log of document ID tracking numbers. The system shall provide a user-friendly log for transmission, printing or export when requested. The system shall provide the ability to retain, archive and purge the print tracking log as defined by organizational policy.		
9.2 Log should contain records to uniquely identify view-only access events.	2008		F249 Match	Enforcement of Confidentiality: The system shall identify all users who have accessed an individual's chart over a given time period.			
9.3 Require EHR system controls on who can electronically export or print from the EHR, reason required, and specific system authorization required.	2008		No Match		S2 The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups including print/export privileges.	No Match	

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-10. Mapping Requirement 10: Patient Involvement in Anti-Fraud to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
10.1 Allow patient to access to their own completed records and release of information (disclosure) log.	2008	Patients can be a potent force in combating fraud. However, they must be given the tools to do so. That is one purpose of an Explanation of Benefits (EOB) notification from a claim. Access to and review of their medical record documentation which was used to generate a claim would be an even stronger tool for prevention and detection of fraud.	Partial Match S1, S2, S3, S12	(If patient access is granted by an organization, S1, S2, S3 & S12 would address access controls and authentication.)	NEW: The system shall grant the patient access to their medical record. (Criteria S1, S2, S3 and S12 would apply)	IN.1.4 Partial Match	Patient Access Management: The system shall conform to entity access control in order for a health care delivery organization to manage a patient's access to his or her health care information.
10.2 Provide patient the ability to comment in the EHR.	2008		No Match		NEW: Adapted from HL7 DC.1.1.3.2 Capture Patient Originated Data: ~~If~~ The system shall ~~-~~provide the ability for direct entry by the patient into their medical record,~~-~~and explicitly label the data as patient entered.	DC.1.1.3.2 Partial Match	Capture Patient Originated Data: If the system provides the ability for direct entry by the patient, then the system SHALL explicitly label the data as patient entered

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-11. Mapping Requirement 11: Patient Identity-Proofing to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
11. Require capability to document/record that identity-proofing was completed and the method used to verify (i.e., check photo ID, prior relationship, or verification of information an individual knows or can produce) consistent with the recommendations of the Confidentiality/Privacy/ Security Workgroup of the American Health Information Community.	2009	One of the fastest growing types of health care fraud is medical identity theft—patients commit fraud by masquerading as another individual in order to obtain medical services. Even if detected, the ramification and liability of this type of fraud is costly. - Provider organizations will be left with unbillable services for the fraudulent individual (or a payer requesting reimbursement for services provided to the fraudster)- Individuals will have incorrect information in their medical and billing record which could negatively impact them in the future (i.e., when obtaining services such as life or health insurance; obtaining equipment or a device in which insurance will only pay once in a lifetime).- Payers reimburse for services not delivered to the insured. To reduce the risk of medical identity theft to all parties, positive identification of an individual prior to delivery of services is crucial. The Confidentiality/Privacy/Security workgroup of the American Health Information Community (AHIC) has identified this as a critical issue and offered	No Match	Note: standards are evolving - monitor AHIC Confidentiality, Privacy, Security workgroup.	NEW: The system shall provide the ability to record that identity-proofing was completed and the method used to verify (i.e., check photo id, prior relationship, or verification of information an individual knows or can produce) consistent with the recommendations of the Confidentiality/Privacy/Security Workgroup of the American Health Information Community.	No Match	

(continued)

Table G-11. Mapping Requirement 11: Patient Identity-Proofing to CCHIT/HL7 Criteria (continued)

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
		their recommendations on handling identity-proofing at the January 23, 2007 meeting. The workgroup defines identity-proofing as the process of providing sufficient information to correctly and accurately establish and verify a patient's identity to be used in an electronic environment. The workgroup outlines three ways identity-proofing can be completed: 1) Validating a government-issued picture ID; 2) Establishment of a durable relationship; or 3) Verification based on information an individual knows or can produce					

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-12. Mapping requirement 12: Structured and Coded Data to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
12.1 The EHR system must have the ability to accept structured and coded data for existing data standards.	2008	Use of advanced analytics and pattern detection is one of the strongest tools to prevent fraudulent behavior. The greater the degree of coding in a record, the greater the ability to prevent fraud.	No Match	Note: CCHIT Comments to the MRET state that structured and coded data is required in each subsequent year on the roadmap. Readily doable using CDA Release 2. Will need clearly defined & broadly accepted standards.	NEW: The system shall have the ability to accept structured and coded data for existing data standards as per the CCHIT Roadmap.		
12.2 Support directly capturing clinical information from the clinician in structured and coded form to the maximum degree possible consistent with the principle of not adversely impacting user productivity.	2008		F67 Partial Match	Manage Clinical Document and Notes: The system shall associate standard codes with discrete data elements in a note.	Manage Clinical Document and Notes: The system shall associate standard codes with discrete data elements in a note. Note: The Roadmap should specify a minimum level of structured and coded input that will increase over time.		

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-13. Mapping Requirement 13: Integrity of EHR Transmission to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
13. Transmit clinical information to other information systems using standards that retain the available level of coding and structure, such as the HL7 Clinical Data Architecture.	2008	Intentional or unintentional modification of records can occur during the transfer from one system to another. Systems must be able to irrefutably ensure that transmission of EHR information has occurred in an unaltered state.	S28 Partial Match	Security Technical Services: The system shall support protection of integrity of all PHI delivered over the Internet or other known open networks via SHA1 hashing and an open protocol such as TLS, SSL, IPSec, XML digital signature, or S/MIME or their successors.	The system shall support protection of integrity (including assurance that EHR data has not been modified during transmission) of all PHI delivered over the Internet or other known open networks via SHA1 hashing and an open protocol such as TLS, SSL, IPSec, XML digital signature, or S/MIME or their successors.	IN.5.1 Partial Match	Interchange Standards: The system shall provide the ability to seamlessly perform interchange operations with other systems that adhere to recognized interchange standards.

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.

Table G-14. Mapping Requirement 14: Accurate Linkage of Claims to Clinical Records to CCHIT/HL7 Criteria

MRET Recommended Requirement	Date Recom-mended	MRET Rationale	CCHIT Requirement No. & Type of Match	2007 Ambulatory CCHIT Function/ Criteria	Proposed Language[a]	HL7 Requirement No. & Type of Match	Sept. 2006 HL7 Function/ Criteria[b]
14. Require a traceable and auditable path from a claim payment or a transmission of a pay-for-performance payment to the clinical documentation supporting it.	2008	The ability to link a claim to the clinical record on which it is based is a fundamental requirement for fraud detection. Systems must be able to irrefutably ensure the linkage of a claim to the clinical record on which it is based.					
14.1 Information transmitted to a claims preparation system will include the document ID tracking number generated in the EHR traceability requirement above.			No Match		NEW: The system shall pass the document ID number for documentation supporting a claim to the claims preparation system (e.g., billing system or directly to the payer).		
14.2 All information transmitted for the purposes of supporting claims or pay-for performance payments will be logged in an audit file that cannot subsequently be changed by a user or administrator of the EHR system. The audit file will include the time at which the submission was created and any relevant document ID tracking numbers generated under the EHR traceability requirement above.			No Match		NEW: The system shall record as an auditable event the point when a claim was generated (if within EHR system) or the point that information was transmitted to a claims preparation system. The system will also record in the audit log the document ID tracking numbers that links the supporting documentation related to the claim generated/transmitted. The system shall provide a user-friendly log for transmission, printing or export when requested. The system shall provide the ability to retain, archive and purge the print tracking log as defined by organizational policy.		

[a]Edits to CCHIT or HL7 criteria shown.

[b]Only cited if there is a gap in CCHIT criteria that is filled by an HL7 criteria.