Written Testimony of Barbara Demster, MS RHIA

1.0 Introduction and Description of Problem

Patient Identity (PI) Integrity is the accuracy and completeness of data attached to or associated with an individual patient. Data must be reliable, reproducible, and sufficient for matching purposes. Completeness refers not only to having adequate accurate data but also to linking or pairing correctly all existing records for that individual within and across information systems and organizations. PI Integrity is of central importance to achieving quality of care, patient safety, and cost control. It is a management challenge with no one simple solution but rather a complex mix of functions and solutions that must be addressed and mastered by and across organizations.

The ultimate goal of PI Integrity is the accurate identification of the patient and linking of all related information to that individual within and across systems. Linking the wrong clinical information to a person not only can cause great personal harm to the patient, but also can result in major costs to the healthcare provider in correcting and mitigating the error. Incorrect information impacts patient safety and compromises quality of care. Good clinical decisions based on bad data become bad clinical outcomes. For example, the wrong patient who received the wrong lens implant must undergo a second procedure to correct it. A third procedure is performed on the correct patient who never got the procedure due to the identity error. In addition to the obvious negative impact on the patient, providers are also negatively impacted in that they must absorb the costs of correcting their mistakes as well as any legal costs involved. There is also the hidden cost of damage to the reputation of the provider based on bad clinical outcomes. Research results can also be impacted by the introduction of corrupted data.

Poor patient identification practices also support perpetration of medical identity theft. "Patients' medical records are altered to reflect diseases or treatments they never had, which can be life threatening if they receive the wrong treatment or find their health insurance exhausted," according to Pam Dixon, founder of the World Privacy Forum.[1] Not only is medical identity theft a lucrative enterprise for the criminally inclined, but the rise in the number of uninsured also correlates directly with the rise in medical identity theft.

The healthcare industry is moving aggressively in expanding the use of electronic health records (EHRs), electronic medical records (EMRs), personal health records (PHRs), and health information exchanges (HIEs). Because of the enormous impact that PI Integrity has on the clinical, financial, and administrative business of healthcare, it is imperative that the quality of an organization's identity integrity be addressed as a major priority within an organization and most certainly prior to sharing data externally with other stakeholders. Stakeholders should require quality data from fellow participants prior to participation in any data exchange.

[1] Bloomberg Businessweek, March 23, 2010

The HIMSS Patient Identity Integrity Work Group has looked extensively at this problem and has documented its assessment in a White paper "Patient Identity Integrity." HIMSS felt compelled to write the paper *now* because of the potential consequences of introducing flawed processes and known errors into a new network through HIEs. HIMSS identified nine key influencers and made 56 recommendations to move the field forward. One of the recommendations is to commission an independent study of available information technology solutions to address an *informed patient identity solution*. As part of a multi-stakeholder coalition, HIMSS is pursuing this action. While this recommendation is a key component in solving the problems inherent in patient identity, all of the recommendations carry some level of impact that healthcare should address. A full description of the problem, along with the detailed recommendations, can be found in the white paper.

2.0 Key Influencers on Patient Identity Integrity

In June 2008, the HIMSS Privacy and Security Steering Committee created a Patient Identity (PI) Integrity Work Group comprised of a diverse healthcare stakeholders and experts to address concerns raised from a variety of sources about the need for guidance in understanding the complex issues surrounding PI Integrity in the real world environment.[2] The HIMSS PI Integrity Work Group published a white paper in December of 2009, "Patient Identity Integrity," that describes the problems associated with Patient Identity Integrity, the factors that influence in this area, and proposed industry actions to help mitigate the issues. (The HIMSS White Paper is submitted with this testimony.)

To solve the problem of assuring a state of high quality PI Integrity, one must look at the entire process of patient identity management (PIM). The Work Group identified nine variables that influence, in varying degrees, the ability to build and maintain a database in a high state of identity integrity. These key influencers are: **industry standards, interfaces, algorithms, unique identifiers, business processes, data accuracy, data quality, training and medical devices**. Poor performance in any one of these functional areas can have serious negative impact on the overall patient identification process.

The paper's Executive Summary describes the major concerns related to each of the nine key influencers. The Work Group made 56 total recommendations for improving the current state of practice across the nine identified key influencer areas. These detailed recommendations can be found in the body of the white paper under the relevant influencer. Belief in the importance of the recommendations to healthcare, coupled with concern that they be implemented in as fast and effective way as possible, the Work Group analyzed the recommendations for the type of action required to make them broadly available to the industry. This paper discusses HIMSS next steps for operationalizing the recommendations.

Many of the recommendations lent themselves to multiple actions and overlapped categories. Thus, the WG identified four major action categories: 1) creation of a Centralized Industry Knowledge Resource for PI Integrity, 2) actions specific to Medical Devices, 3) Industry Actions, and 4) Government Interface and Actions. The four action categories are discussed below.

2.1. Creation of a Centralized Industry Knowledge Resource for PI Integrity

[2] The list of work group members can be found in Appendix F of the HIMSS PI Integrity White paper.

The vast majority of the HIMSS white paper recommendations fell into the "create an industry resource" category indicating an identified need for access to existing knowledge about PI integrity, guidance documents, tools, models, best practices and educational resources.

Working with the HIMSS Privacy and Security Toolkit Task Force, the PI Integrity Work Group plans to establish a reference site as a free resource through a dedicated Patient Identity Section in the HIMSS Privacy and Security Toolkit. This site will be a central repository for information on the topic of Patient Identity Integrity. Existing content will be combined with new content identified from the gaps and recommendations reported in the white paper. Comprehensive content areas will include **Model Business Practices, Guidelines and Training Resources** with a target audience of all management levels, front line staff in Patient Access, HIM, IT, Registration, Scheduling staff, clinical departments, among others. Resources will be newly developed or examples of real implementations at successful model organizations. The initial content outline is discussed below. Initial sections will include the following information that specifically addresses the recommendations and gaps reported in the HIMSS white paper. The goal for completion of these Toolkit content items is June 30, 2011.

2.1.1. Security Safeguards

This section of the Toolkit will address specific recommendations related to security safeguards. Guidelines will be provided to assist providers in how to ensure adequate security controls and processes are in place and embedded in the workflow to assure minimal risks to privacy. Also included will be role-based security training requirements as responsibilities and capabilities vary by role in an organization.

While the existing HIPAA security regulations are considered to be adequate, the HIMSS work group identified their poor implementation and enforcement as a threat to PI integrity. Thus, the group recommended greater guidance in the area of security to ensure PI integrity. Effective security controls and processes must be embedded in the workflow. There is a great need for guidance in how to incorporate the controls into the workflow and business processes for patient identification, including role-based staff training requirements.

The work group also recommended a strong enforcement presence to reinforce provider understanding of the importance of security and to provide them with effective tools to accomplish full integration into their business processes. This section will provide guidance in those areas.

2.1.2. Model Interface Protocols

Major improvement in the manner in which computer systems share information is being achieved. Notably, Integrating the Healthcare Enterprise (IHE) initiative promotes the use of established standards and has developed profiles for patient identification, although some issues still exist in the area of patient privacy. A major problem exists in implementation of interfaces at the local level. The number (30 to 60 in an average hospital) and complexity of applications and systems being interfaced creates a daunting task for staff to implement and maintain. Too

frequently this is left solely to IT staff; yet, correctly and accurately mapping data to patients across the systems requires both IT and domain expertise. The lack of domain expertise in the process impacts the effectiveness of many IT installations. Collaboration between information management, IT, and other domain experts in the development of thorough testing plans would improve the efficiency as well as the effectiveness of the systems.

In the HIMSS PI Integrity Toolkit, guidance will be provided to help ensure that information system employees at the local level are properly trained in understanding patient identity and their role in ensuring its integrity through creation of interfaces that transmit patient data between applications. This section will provide model testing protocols, procedures, tools including test scripts to help ensure that a message sent is the message received and arrives at the intended destination without error. Guidance will be provided to bring attention to major local interface issues such as the downstream impact of patient identification standards. It will provide protocols for testing the patient identification standards and profiles in the organization's environment which will include a multi-disciplinary approach since so many different areas of an organization are impacted by patient identification.

2.1.3. Metrics

This section of the Toolkit will provide tools and use cases for managing PI integrity in a variety of healthcare settings. Tools and use cases for effective matching will include: accepted formulas for computing duplicate record rates and duplicate creation rates; guidance on selection of search thresholds and their implications; guidance on selection of record auto-linking minimums and their implications; guidance on maximum allowable duplicate record rates and formulas for their computation, among others.

There are no formal national standards accepted across the industry for measuring effectiveness of patient identity management. There is a need for development of standard measures, tools and use cases for measuring effective matching, both by the technology in play as well as the employees responsible for the matching process. This includes guidance on measuring and reporting error rates in healthcare databases, and identifying an acceptable error rate. Manufacturing has sophisticated methods for measuring its tolerance for error on the production line. The consequence of an identity error can be fatal, yet the healthcare field has no formal way of measuring its error rate. The public would not accept a 97% accuracy rate for successful landings in the aviation industry. Standard formulas are needed for computing duplicate record rates, duplicate creation rates, search threshold minimums, record auto-linking minimums and maximum allowable duplicate record rates, among others. These measures can be incorporated into employee performance monitoring and used by management to monitor the effectiveness of their PI program. Metrics are frequently driven by context, therefore use cases are needed to describe any metrics variances between particular settings such as an enclosed enterprise versus an HIE.

2.1.4. Model Data Practices

The processes surrounding technology solutions are critical to the success of a solid PI Integrity program. There is a lack of adequately defined business process standards or guidance that surrounds proper patient identification. Data accuracy and data quality are critical business processes, yet in healthcare, there are no standards for data accuracy or data quality. This section of the Toolkit will provide policies and procedures for best practices in a sustaining a PI Integrity program. Initial content responsive to the recommendations will include discussion of the minimum data elements required to maintain PI Integrity in record matching algorithms; the importance of creating and maintaining a data dictionary; model procedures for the collection, re-entry validation, input, and information query, use of lookup entries and newer technologies.

The majority of recommendations from the white paper revolved around data practices. There is no core data set or minimum defined elements required to provide consistency in record matching algorithms while minimizing privacy impact. Definitions of data elements can vary within an enterprise, not to mention across organizations in information exchange. This section will provide industry guidance on the process that providers and health information exchange organizations should follow to resolve potential duplicate records within their databases. Model data practices will include recommended data elements and data dictionary along with model procedures for data collection, patient re-entry validation, input and query of information, use of lookup entries and newer technologies.

Explicit organizational guidelines for data stewardship and data governance that reach beyond patient identification are critical to the success of patient identification processes. Examples of tools and models required for a comprehensive PI Integrity program include: standardized corrective action required by ineffective business processes or human error; standardized procedures for the collection, input, and query of information; staff training on interview techniques and to verify data elements before entering them to prevent assumptions among other.

2.1.5. Model Monitoring Reports

This section will provide model reports for managing a PI Integrity program. Reports are key business practices that should be designed to support the monitoring of data accuracy and staff performance. Measurement of patient identification accuracy should be through standard reports structured to monitor them. Model reports will provide varying views to include data accuracy, pattern analysis and trending by individual (e.g. registrar or scheduler), location (work area or department), as well as overall organization performance. Areas that fail to meet expectations or that have not had appropriate historical practices must be corrected. This may involve implementation of new IT paired with effective procedures and ongoing training. Any successful long-term solution must incorporate people and processes along with technology. This section will provide guidance on model monitoring reports and corrective action models.

2.1.6. Executive Level Education

This section is focused on education of the executive suite in why it makes good business to support, promote, and – most importantly – fund a quality patient identity program. This includes its impact on quality care, patient safety, and how it impacts the financial bottom line.

Findings from the 2010 HIMSS Security Survey indicate that there is a need for education in having an active identity management program. The survey asked respondents how duplicate records were identified in their master person index. Fifty-six percent reported having a formal reconciliation process while another 27% reported an informal manual process. Five percent responded that they had no process for managing duplicate records. [3]

This section will include education on organizational best practices which start with an organization's commitment to accurate patient identification. They include the need for quantifiable expectations and performance standards, data governance stewardship, training and administration of all intake and scheduling areas including appropriate compensation, recognition, and professional certification in those areas. Executive level support for a multi-stakeholder administrative group that identifies problem areas, monitors relevant data, prioritizes corrective actions, and practices structured, ongoing communication is the foundation. Emphasis for this group must include ensuring adequate tools and resources, and process support, including initial and ongoing competency-based training.

2.1.7. Existing Literature/Publications

This section will be a general repository devoted to articles, documents, and publications related to the topic of patient identity integrity.

2.2. Medical Devices

Medical Device incompatibility is a major problem in the PI Integrity sector. Neither hardware connections nor data are compatible. Data incompatibility due to no common format means lack of data interoperability for exchanging data. Hospital-based devices historically retain the information in the machine and have been designed as one machine to be used on many patients. Home monitoring devices are designed for personal use by one patient and have made great advances in addressing and communicating information. The 16 recommendations related to Medical Devices have been referred to the HIMSS Medical Device Task Force. The PI Integrity WG believes that Medical Devices need standardization of their data and technology as quickly as possible as well as the incorporation of algorithms to promote accurate record linking.

2.3. Industry Actions

Two specific recommendations related to promotion of standards and models within healthcare. The first recommendation relates to requiring use of HL7 and IHE standards (ATNA Integration Profile) and vendor compliance through an HHS certification process. The second involves encouraging acceptance

[3] 2010 HIMSS Security Survey

and dissemination of the Toolkit Models, Best Practices, and resources among industry and with the National Institute of Standards and Technology (NIST), government actions and activities.

3.0 Rand Report: "Identity Crisis"

In late 2008, the Rand Corporation published a monograph titled "Identity Crisis: An examination of the costs and benefits of a Unique Health Identifier for the U.S. Health Care System." The monograph "examines the operational advantages and disadvantages, compares the errors, examines the costs, and discusses the privacy issues associated with the (Unique Patient Identifier) UPI and its alternatives."

Analyzing an 80-million record demographic database for a comparative analysis of the effectiveness of the UPI versus statistical matching, the researchers concluded the following:[4]

- Broad Adoption of a UPI Should Enhance the U.S. Health Care System
- A Hybrid System Utilizing Both Statistical Matching and a UPI Will Be Necessary for the Foreseeable Future
- Security and Privacy Could Be Strengthened with a UPI
- Costs of a UPI Are Significant, but Probably Much Less Than the Value Associated
- with Error Reduction, Efficiency, and Interconnectivity of the Health Care System

The report went on to state: "These issues should be the subject of open study and debate in the vitally important process of developing the best interoperable U.S. health care system and reducing the errors and inefficiencies in that system. Continuing *de facto* endorsement of statistical matching as the only practicable approach to linking patients to their electronic health records will inhibit the effective development of the national health information network."[5]

These conclusions work in concert with the findings of the HIMSS white paper although RAND and HIMSS used entirely different approaches, the former more quantitative in the analysis of a large database and the latter more observational and qualitative through the use of industry experts. Despite the differences in approach and focus of study, the findings and conclusions are supported by both reports.

4.0. Questions for Testifiers:

4.1. Question 1: What are your standards for identifying individuals?

As discussed in the HIMSS white paper, identification of individuals is a complex process comprised of many components, reflecting many situations and settings, and requiring differing standards and practices. The recommended standard for identifying individuals is to leverage the nine key influencers in the HIMSS white paper to achieve optimum results in patient identification. Unfortunately, nothing is standard when it comes to patient identity. While there are many recommendations and models for

[4] Rand Report "Identity Crisis" p. xvii
[5] Ibid.

patient identity and record linking, we do not have any true standards used universally across providers and vendors in the industry. Data practices vary from provider to provider as they use their locally determined standards.

This is particularly troubling as we move to HIEs and the exchange of information across disparate entities and systems. HIEs need to set some threshold of tolerance around data quality and patient identity data elements which should then roll downhill to the provider.

The HIMSS white paper identifies two major gaps in existing standards for patient identity. The first relates to a need for data standards for effective identity resolution. The second relates to standards to create more transparency in the effectiveness of the variety of algorithmic matching approaches currently in use today. There is a major conflict between vendor reports of successful identity matching results and MPI cleanup services findings that anecdotally report error rates up to 40%.

Organizations with active dedicated duplicate management programs that address the key influencers report reduction in duplicate rates as from 25% to as low as 0.02% (99.98% duplicate free). This would suggest a need for standards for business processes, management infrastructure, and oversight.

4.2. Question 2: How can you be sure that you are accurately linking a patient with his/her data?

The best way to know for sure that you are accurately linking a patient with his/her data is to have the patient in front of you for a real-time interview utilizing strong business processes not only to validate the identity of that person to ensure they are who they claim to be but also to ensure they are then accurately entered or matched in the system. Unfortunately, the patient is not available most of the time when these activities are required.

The best technological solutions for accurately linking are considered to be biometric solutions (such as retinal scans, finger prints, and palm blood flow, among others) and use of a Unique Identifier. Otherwise, there are too many opportunities for inappropriate linking which must be addressed through business process. Some common examples of those are:

- Laboratory technician enters reference lab specimen information faster than the technology can accept and enters demographic information into previous entry's record.
- Updating of pseudonamed records such as Jane or John Doe, Baby Up For Adoption (BUFA baby), newborns (Babyboy Jones), among others, and the end-user chooses the wrong patient record.
- Medical ID theft – sharing insurance information, SSNs, etc.

Another confounder in the process is that historical conversions of databases cannot be guaranteed in their accuracy. There is a great potential for records to have been comingled or overlayed (where two different individuals' records have been merged into one). These types of errors are frequently found by the patient or provider who stumbles into it by chance when reviewing/using the information in the record, such as “I've never had diabetes” or “It’s the right leg, not the left leg...”

Bottom Line: For the best matching outcome, use a comprehensive approach to identity management, including all of the nine key influencer areas

4.3. Question 3: What problems are you having with patient-matching, internally and/or for information exchange? What is the source of those problems?

The biggest challenges to healthcare organizations as well as HIEs are data management processes to eliminate duplicates and overlays. Without identity integrity, information pertaining to one individual may exist in one or multiple databases where it resides as a "duplicate," inaccessible or unknown to those needing to see the complete or most current picture. Conversely, information on two individuals may be combined erroneously into one record called an "overlay." The source of these common problems can be traced back to the nine key influencers as mentioned in the HIMSS white paper (industry standards, interfaces, algorithms, unique identifiers, business processes, data accuracy, data quality, training and medical devices). The absence of a strong patient identity management program can result in:

- Uninformed or marginalized clinical decision-making that impacts quality outcomes and patient safety;
- Poor utilization of healthcare resources leading to repeated tests or procedures due to lack of access to existing reports or results;
- Increased costs associated with identity errors and their mitigation;
- Inability to drop a bill to collect payment or missed billing opportunities such as when lab results are posted to an old account or wrong account; and,
- Manipulation of the system for illegal purposes such as drug seekers, drug diversion or medical identity theft, to name a few.

The problem with information exchange is that a local provider system with a poorly maintained or "corrupted" master person index (MPI) will proliferate the corrupted data and contaminate all of the other systems to which it links. In an information exchange, a poorly managed provider system transmits inappropriate, inaccurate information to other provider participants who are depending on that information to make good clinical decisions. This can be catastrophic to the patient from the standpoint of direct treatment implications as well as the daunting challenge of correcting their record. This proliferation of corrupt data can also be highly detrimental to an HIE by undermining provider confidence and trust in the data in the exchange. Erosion of trust in the data will erode participation in the exchange.

These events have brought PI Integrity to the forefront because of its critical importance to the successful implementation of these information systems. HIEs magnify the problem for several reasons:

- They do not have control of the patient identity data capture process,
- They receive data from many different provider MPIs and the data fields being sent to the HIE are frequently inconsistent, and
- They don't control the interfaces coming into the HIE's database.

Since a major portion of the activities of an HIE involve the exchange of clinical information between independent (and therefore heterogeneous) entities, these issues create significant additional stress on the HIE's ability to effectively maintain their system with high data integrity.

Question 4.3.a. How do you handle patient matching problems (wrong/ambiguous match)?

Organizations successful in patient identity management provide a robust duplicate management process to resolve wrong or ambiguous matches. As mentioned above in question 4.1., organizations with active dedicated duplicate management personnel report duplicate rates as low as 0.02% (99.98% duplicate free). To be effective, these individuals must understand both the user and the technology side of the equation to track errors back to its source. Remediation processes with root cause analysis must be in place to correct the error itself as well as eliminate where possible the source whether it be technology (such as an interface issue, algorithm) or human (such as a poorly trained or performing registrar).

Question 4.3.b. What should be done when there is no match although one was expected?

One of the problems with probabilistic and deterministic matching algorithms is that their matching thresholds are set too high. Anecdotal findings from cleanup services report that the largest concentration of duplicates often reside in the range of 45% to 60% data match yet most organizations set their record matching thresholds to only report matches above 85% to keep from inundating their users with potential duplicates.

Organizations must establish business processes to research and rectify situations where a match is expected, but not found. This includes strong and flexible information gathering as well as query processes which provide additional creative ways of searching the database. The duplicate may be residing in the range below the established threshold. The best solution is to start with a clean database and implement strong management processes to maintain it.

Question 4.3.c. In your experience, what are the consequences of a wrong match? – to patient safety, privacy

Clearly the worst case scenarios are death, wrongful physical (and mental) invasion up-to-and-including dismemberment due to identity error. More frequent are the near misses or inappropriate clinical decisions based on someone else's information. When a wrong match is overlayed, at least two individuals are affected. Patient B (the wrongly selected) has suffered an invasion of privacy by having his/her personal information exposed to Patient A (the "correct" patient) and his/her treatment staff. As Patient A's information is comingled with Patient B's information, both patients are at risk for inappropriate clinical decisions made based on the other's information. This information can now be proliferated through information exchange making it more difficult to "correct" the record and have a wider range of impact on both patients. Additionally, individual healthcare organizations commonly do not have processes in place to "correct" electronic health records.

Question 4.4. What level of accuracy do you establish for patient matching

This is a difficult question to answer. Clearly, the desired level of accuracy is 100% in patient matching.

If we are talking about algorithm matching thresholds, as mentioned above in question 4.2, one of the problems with probabilistic and deterministic algorithms is that their matching thresholds are set too high. Cleanup services report consistent findings in their database analyses that the largest concentration of duplicates often resides in the range of 45% to 60% identity data match. Yet most organizations set their record matching thresholds to only report records that have data matches above 85% to keep from inundating their users with potential duplicates.

If we are talking about a maximum allowable duplicate record rate or duplicate creation rate within a database, we would expect a very high level of accuracy and thereby very low error rate. According to the Airline Pilots Security Alliance, there are 28,000 flights per day in the United States with approximately 5,000 airborne at any one time. We would not accept a 98% successful daily landing rate from the airline industry. Such a percentage would translate to 560 failed landings per day. Knowing the impact an identity mismatch can have on quality care, patient safety as well as unnecessary cost to the institution, healthcare and society's tolerance for identity error should also be quite small.

Institutions with active duplicate management programs report duplicate error rates as low as .02%, or successful matches at 99.98%. Accurate patient matching can be accomplished when using a total identity management approach.

4.5 What lessons learned do you have from solving this problem?

The most important lesson learned is that there is not a single magic solution to patient identity integrity. A comprehensive approach must be taken that includes both technology and business processes. For effective identity matching, the nine drivers that influence patient identity integrity must all be addressed and operating at a high functional level. The interaction and interdependence of these influencers are additive in nature to overall matching outcome. Failure in any one area can bring down the effectiveness of the entire identity management process.

Senior management must champion and expect quality patient data. This means educating themselves on the implications to their organizations of good data and bad data. Identity integrity costs money, and is labor intensive. Management must understand the costs of bad data as well as the cost savings of good data. Funding the necessary internal processes to support a quality data and identity management program must become a necessary part of doing business.

The creation of duplicates cannot be prevented entirely because humans are involved, as patients, as registrars, as clinicians, as IT staff, among others. Management must build an infrastructure that minimizes the risks while optimizing the opportunities for influencing duplicate creation and elimination.

There will always be a need for algorithms. However, we need more independent study and transparency into their actual effectiveness.

A unique health identifier greatly enhances the opportunity for accurate matching yet must be protected from use for any reason other than healthcare. The RAND analysis of an 80-million-record demographic database indicated that an error-free composite key made up of name, date of birth (DOB), zip code, and last 4 digits of the SSN (as a unique identifier) would be required to unambiguously identify all patients. RAND found that removing the partial SSN from the key created nearly 1,000 false-positive matches in the database. Larger health record databases, such as those of a national or large regional network, almost certainly require a unique identifier to avoid false-positive errors[6]

While there are historical concerns with the idea of a unique patient identifier, we must recognize the potential of this implementation to eliminate patient data matching errors, increase patient identity integrity, bring down costs, and perhaps even *enhance* privacy.

4.6 What are the cost implications of various solutions?

In terms of a unique identifier solution, the biggest problem when talking about the cost is whether you are only talking about the costs of the centralized system, or whether you are talking about the cost to every provider for such items as a bar code reader, equipment to print out and deliver an ID card to every patient, among others.

Additional cost implications revolve around the identity management holistic approach's base costs to the provider for maintaining a clean MPI and a high state of identity integrity. These costs would include: initial database analysis, MPI cleanup, then sustaining an ongoing data maintenance and identity management program, hiring and paying adequate wages to qualified staff for patient intake as well as data management, ongoing education and training of all staff (patient access & registration, scheduling, IT, HIM, billing, lab, radiology, all departments, and the C-Suite among others) in identity management best practices. Without an ongoing identity management program, the database will devolve into its original state prior to the cleanup.

The RAND report provides cost data and should be referenced for the cost detail breakdown for centralized systems. It is important to note that the RAND study estimates that the annual *savings* from implementing a unique identifier just from reduced adverse events and reduced duplicate testing would be $8.5 billion annually.

4.7 What should ONC do to address patient matching problems in information exchange

The following actions by ONC would greatly impact for the better the quality of patient matching in information exchange:

- Facilitate research around algorithm effectiveness to promote transparency in this area. Using study results, recommend algorithm standards including search threshold minimums and record auto-linking minimums.

[6] Identity Crisis, RAND Corporation, 2008

- Work to promote standards and regulation for data capture, patient identity metrics, and business processes that influence patient identity. This would include adoption of an industry standard method of computing duplicate record rates in MPI databases and a standard formula for computing the "creation" rate of newly created duplicate records.
- Support funding for development of national best practices, business models, case studies, and tools surrounding the nine key influencers of patient identity.
- Support strong enforcement of the privacy and security regulations.
- Support the required use of HL7 and IHE standards (ATNA Integration Profile) and vendor compliance through HHS Certification.