ANALYSIS OF UNIQUE PATIENT IDENTIFIER OPTIONS

FINAL REPORT

November 24, 1997

Prepared for THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
by Soloman I. Appavu

Table of Contents

Part One: Executive Summary

Introduction

Patient Identifiers are vital for healthcare organization's day to day operations such as the delivery of care, administrative processes, support services, record keeping, information management, and follow-up and preventive care. The revolution, currently taking place in our national healthcare delivery system and in the computer and telecommunication technologies, has expanded the scope of these functions across multiple organizations spread around the nation. In addition, patients are mobile, visit multiple providers and treated by multiple organizations. Therefore, to support the continuum of care, it is necessary to uniquely identify patients across multiple providers and access their information from multiple locations.

The current method of patient identification involves the use of a medical record number, issued and maintained by a practitioner or a provider organization. This number is based on an institutional Master Patient Index (MPI) and the numbering system is specific to the issuing organization. Different provider organizations use different numbering systems. Patients receive multiple Medical Record Numbers, each issued by the organization that provided them care. These numbers provide unique identification only within the issuing organization. A Patient Identifier that is unique only within a provider organization or a single enterprise is inadequate to support the national healthcare system. In order to uniquely identify an individual across multiple organizations, a reliable Unique Patient Identifier is required. The Health Insurance Portability and Accountability Act of 1996 requires the Secretary of Health and Human Services to adopt standards for Unique Health Identifiers to identify individuals in addition to providers, health plans and employers. The industry has put forth several options for the Unique Patient Identifier; this report examines their effectiveness and readiness.

Objective

The objective of this study is to perform an analysis of the various Unique Patient Identifier options that are available for use in healthcare. The result of this analysis will facilitate and support the recommendation to be made to the Secretary of HHS by the NCVHS.

Method of Analysis

In order to evaluate all functional and operational aspects of the various Unique Patient Identifier options, this analysis employs a two step process. In the first step, various issues surrounding the Unique Patient Identifier including its required characteristics, capabilities, components, functions and use are analyzed. In the next step, each Unique Patient Identifier option is analyzed individually. The analysis was based on a set of criteria including ASTM criteria for a Universal Healthcare

Identifier. ASTM's "Standard Guide for Properties of a Universal Healthcare Identifier (UHID)" includes thirty (30) conceptual characteristics for evaluating identifier candidates. However, it does not address implementation issues and operational characteristics. Therefore, in order to fully evaluate the Unique Patient Identifier options beyond a conceptual level and verify their compliance both with functional and operational capabilities required in a live day-to-day patient care environment, the options are analyzed based on the following evaluation criteria:

1. ASTM's Conceptual Characteristics

2. Unique Patient Identifier's Operational Characteristics

3. Unique Patient Identifier's Components

4. Unique Patient Identifier's Basic Functional Requirements.

Report Template

For the sake of consistency, a common template consisting of the following categories is used to analyze each option:

I. Description of the Option
II. Author/Proponent of the Option and Documentation
III. Compliance with ASTM's Conceptual Characteristics
IV. Compliance with Operational Characteristics
V. Compliance with Unique Patient Identifier Components Requirements
VI. Compliance with Basic Functions Requirements
VII. Strengths and Weaknesses
VIII. Potential Barriers and Challenges to Overcoming the Barriers.
IX. Solutions to the Barriers.

Functions and Objectives of Unique Patient Identifier

The four (4) basic functions that a Unique Patient Identifier must support are:

1) Positive identification of the individual:

a) for delivery of care (e.g. diagnosis, treatment, blood transfusion and medication)

b) for administrative functions (e.g. eligibility, reimbursement, billing and payment)

2) Identification of information:

a) Identification to access patient information for prompt delivery of care, coordination of multi-disciplinary patient care services during current encounters and communication of orders, results, supplies, etc.

b) Organization of patient care information into a manual medical record chart or an automated electronic medical record for both current and future use

c) Manual and automated linkage of various clinical records pertaining to a patient from different practitioners, sites of care and times to form a lifelong view of the patient's record and facilitate continuity of care in future

d) Aggregation of information across institutional boundaries for population-based research and planning

3) Support the protection of privacy and confidentiality through, accurate identification (explicit identification of patient information) and dis- identification (mask/encrypt/hide patient information).

4) Reduce healthcare operational cost and enhance the health status of the nation by supporting both automated and manual patient record management, access to care and information sharing.

Required Components of Unique Patient Identifier

A Unique Patient Identifier must include components that will provide it with the necessary functional capabilities. Each identifier must be supported by adequate identification information of the individual it identifies. Such information must be current; indexed and stored properly. The identification process includes searching MPIs, matching identifiers and verifying information. Depending on the identifier's scope and level of use, the search processes can range from a single provider organization to the entire national healthcare system with the possibility, in future, to expand worldwide. Therefore, the Unique Patient Identifier requires a robust technical and administrative infrastructure. The following six (6) components are integral parts of the Unique Patient Identifier. They must work together in order for it to perform its functions and fulfill its objectives:

1. An Identifier (numeric, alphanumeric, etc.) Scheme
2. Identification Information
3. Index
4. Mechanism to hide or encrypt the Identifier
5. Technology infrastructure to search, identify, match, encrypt, etc.
6. Administrative infrastructure including the Central Governing Authority.

Privacy, Confidentiality & Security

Privacy, Confidentiality and Security of Patient Care Information

Privacy, in the healthcare context, amounts to the freedom and ability to share an individual's personal and health information in confidence. Confidentiality is the actual protection such information receives from the provider organizations. An individual's personal and health information include those that were supplied by the individual and those observed by the care giver during the course of the delivery of care. Security is the measure that an organization has employed to protect the confidentiality of the patient information. In essence, privacy of an individual's health information depends on the level of confidentiality maintained by organizations which in turn, depends on the security measures implemented by them. Respect for the privacy and confidentiality of patient information must be adopted and fostered as an essential organizational policy and culture. Security measures that are failsafe must be utilized. Yet, the organizational security measures can work only within the walls of the organization and among its employees. Protection outside the provider organization will require federal legislative measure in addition to an organization's security measures. Therefore, protecting the privacy of patient information is a joint responsibility of individuals, organizations and the nation as a whole; appropriate effort must be put forth by all of them.

The Privacy and Confidentiality Challenge

The privacy and confidentiality of patient care information is a difficult challenge facing the entire healthcare industry and cannot be ignored. The following measures are necessary to overcome this challenge:

1) A judicious design of the identifier

2) Organizational security measures to control access

3) Uniform federal/state legislation

4) Developing security policies and instilling responsibility among individuals.

1) Judicious Design

Identifier design should separate the identification function from the access control function. The identifier's capability must be limited to identification only and the access control function must handle access to all information. The access control will verify the authentication of the system user, check the access privileges of the requestor and maintain an audit trail of all activities. The identifier must be designed to be unique and supported by a set of standard/uniform identification information. The design must also include the capability to store as well as communicate the identifier in an encrypted format.

2) Organizational security measures to control access

Appropriate organizational policies and procedures to protect the patient care information must be maintained by healthcare organizations. A failsafe access control mechanism including software access security, physical access security, encryption protection and an authentication mechanism must be in place to prevent

unauthorized access and ensure legitimate access. The security measures include audit trails for tracking inappropriate access and preventive steps against possible misuse. These protective measures must be evaluated on an ongoing basis and improved continuously.

3) Uniform Federal/State Legislation

Uniform federal and state privacy and confidentiality legislation is required to assure the privacy and confidentiality of patient care information beyond the organizational boundaries. Such legislation must protect the Unique Patient Identifier from misuse, and prevent unauthorized access to patient information and illegal linkages of confidential information to cause harm.

4) Developing Security Policies and Instilling Responsibility Among Individuals. Employees and others who use patient care information have a responsibility for its security. Therefore, individual responsibility for the privacy and confidentiality of patient information must be instilled through staff and user training, education and reinforcement among the users and consumers.

Unique Patient Identifier Options

There are six (6) options for the Unique Patient Identifier, three (3) for Non Unique Patient Identifiers and five (5) as alternatives to Unique Patient Identifier.

Unique Patient Identifier Options

1. Social Security Number
2. ASTM Sample UHID Implementation
3. Patient Identification Number based on Bank Card Method
4. Model UPI based on Personal Immutable Properties
5. Lifetime Human Service and Treatment Record (LHSTR) Number based on the Birth Certificate
6. Biometric Identification

Non Unique Patient Identifiers Options

1) Medical Record Number
2) Medical Record Number with a Provider Prefix
3) Cryptography-based Identifier

Alternatives to Unique Patient Identifier

1. Manual Process
2. CORBAMed Person Identification Service
3. HL7 MPI Mediation
4. FHOP's Standard Data Set as Common Patient Identifier
5. Directory Service.

Result of the Analysis

The outcome of this analysis is summarized in two parts:

1) general findings relating to Unique Patient Identifier requirements, functions, characteristics, components and capabilities

2) Unique Patient Identifier options' compliance with conceptual characteristics, and operational and components requirements.

I. General Findings

GF1. Patient Identifier is an Integral Part of Patient Care

Patient Identifiers are an integral part of the process of delivery of care. Reliable Patient Identifiers are mandatory for sensitive procedures, such as blood transfusion, invasive testing, surgical procedures and medication administration. They are routinely used for 1) ordering and reporting the results of tests, procedures and medications, 2) coordinating the multi-disciplinary patient care delivery processes and 3) managing all administrative functions, such as scheduling, billing, coordination of benefit, etc.

GF2. Patient Identifier is an Integral Part of Patient Information

Patient Identifier is an integral part of the patient care information. Clinical documentation including results, observations, diagnosis, procedures, medication, progress, outcomes, etc. are all based on the Patient Identifier. It is vital for the management of automated information and manual medical record functions including compilation, filing, storage, retrieval and communication. It is mandated by regulatory authorities as a component of the medical record.

GF3. The Need for a Unique Patient Identifier is Urgent and Essential

The continuum of care across multiple providers, access to information from multiple care settings that is required during the delivery of care, and the retrieval and assembly of relevant patient care information from past episodes of care across different times require the use of a Unique Patient Identifier. The identifiers being currently used are not unique across the national healthcare system. Lack of a Unique Patient Identifier presents significant problems in 1) accessing and integrating information from different providers and provider computer systems, 2) aggregating and providing a lifelong view of a patient's information and 3) supporting population-based research and development. The need for a Unique Patient Identifier is, therefore, vital and urgent.

GF4. Industry pursues an aggressive solution for a Unique Patient Identifier

In response to the urgent need for a Unique Patient Identifier, the industry has come up with a total of 12 new proposals for the Unique Patient Identifier. The proponents include provider organizations, healthcare professionals from different disciplines, software developers, standards developing organizations, information technology professionals, industry consortium and professional organizations.

GF5. Privacy, Confidentiality & Security Do Not Preclude the Use of Unique Patient Identifier

The privacy and confidentiality of patient care information is a difficult challenge facing the entire healthcare industry and it cannot be ignored. A Unique Patient Identifier is an integral part of the patient care information. Therefore, it requires the same confidentiality and security protection as the patient care information itself. The privacy, confidentiality and security requirements do not preclude the use of a Unique Patient Identifier. In fact, the Unique Patient Identifier can help meet these requirements by standardizing and strengthening access control, and eliminating the repeated use of personal identification information. Additional measures to fully and effectively address the privacy concerns include: federal legislation, appropriate organizational policies and procedures, access control, audit trails for tracking inappropriate access, public education and continuous evaluation and improvement of these protective measures.

GF6. A Judicious Design of the Unique Patient Identifier Can Fulfill the Patient Care Need and Protect the Privacy and Confidentiality of Patient Information

Unique Patient Identifier requires a design architecture that will keep the identification of patient care information and its access as two distinct and separate functions within healthcare. The identifier's role is limited merely to identify the patient record by accessing only the identification segment of the patient record and not its content. Access control deals with the authentication of the user (e.g. validation of user ID and password), verification of access privileges, audit trails, physical security, etc. It must be supplemented by organizational policies and procedures, and federal legislation.

GF7. Effective Ongoing Organizational Measures are Required to Support Patient Identification and Confidentiality

The judicious design discussed above must be supplemented by appropriate ongoing organizational measures to protect the patient care information. A failsafe access control mechanism including software security, physical access security, encryption protection and an authentication mechanism must be in place to prevent unauthorized access and ensure legitimate access. The security measures include audit trails for tracking inappropriate access and preventive steps against possible misuse. They must be evaluated on an ongoing basis and improved continuously.

GF8 Uniform Federal/State Legislation is Required to Protect the Privacy and Confidentiality of Healthcare Information

In order to ensure the privacy and confidentiality of patient care information beyond organizational boundaries, uniform federal and state privacy and confidentiality legislation is required. Such legislation must protect the Unique Patient Identifier from misuse, prevent unauthorized access to patient care information, illegal linkages and discrimination based on patient care information.

GF9. Individual Responsibility Must be Instilled Through Education

Protection of patient care information is also the responsibility of individuals that

handle them. Therefore, individual responsibility for the privacy and confidentiality of patient information must be instilled through staff and user training, education and reinforcement among the users and consumers. Public education of the value of privacy and confidentiality of healthcare information and the legal consequences of violation must be provided nation-wide.

GF10. Unique Patient Identifier Requires an Issuing Authority

The issue and maintenance of the Unique Patient Identifier, the identification information and their use need to be handled either under a centralized or decentralized administration. The ASTM Standards Guide requires a Central Trusted Authority for this purpose. Example of available options are Social Security Administration and the United States Postal Service. The LHSTR Number proposal recommends the creation of a United States Vital Health Records Trust for this purpose.

GF11. Unique Patient Identifier Prevents Exposure and Protects Patient's Privacy

A Unique Patient Identifier eliminates repetitive use and disclosure of an individual's personal identification information (i.e. name, age, sex, race, marital status, place of residence, etc.) for routine internal and external communications (e.g. orders, results, medication, consultation, etc.) and protects the privacy of the individual. It helps preserve the patient anonymity while facilitating communication and information sharing.

GF12. Unique Patient Identifiers help Standardize the Method of Accessing Patient Care Information

The use of a Unique Patient Identifier to access patient care information helps standardize the access method and enable organizations to use a single point of access. The direct use of the patient demographic information for the purposes of identification will increase the level of exposure and subject the patient to unnecessary privacy risks. The use of non-standard access methods instead of the Unique Patient Identifier method will be difficult to control and monitor. Therefore, it will also increase the potential for the violation of privacy and confidentiality of patient information.

GF13. Unique Patient Identifier Strengthens Access Control to Protect the Privacy, Confidentiality and Security of Health Information

The single point of access and the standard access method enable organizations to plan and implement the necessary access control. They can monitor the access and continuously improve and strengthen the access control with appropriate measures. A valid Unique Patient Identifier provides both the necessary focused control as well as timely and reliable access.

GF14. Multiple Identifiers Inhibit Timely Access

Use of multiple identifiers for the same patient keeps the information fragmented and isolated and makes the timely access to information difficult for care providers from other locations. It may be difficult and cumbersome for unauthorized linkage,

but by the same token it also hurts legitimate purposes such as timely access to information and timely delivery of care.

GF15. Access Security Controls the Privacy and Confidentiality, and not the Identifier

The role of access security is to grant access for authorized use and prevent unauthorized use. The role of a Unique Patient Identifier is to assist the authorized use by accurately identifying the patient and his/her information.

GF16. Unique Patient Identifier is Made Up of Six (6) Critical Components

Unique Patient Identifier is made up of six (6) components essential for its performance. They are:

1. Identifier (numeric, alphanumeric, etc) Scheme

2. Identifying Information

3. Index

4. Mechanism to hide, or, the tool to encrypt the Identifier

5. Technology infrastructure including the software, hardware and communication technologies to search, identify, match, encrypt, etc.

6. Administrative infrastructure including the Central Governing Authority.

These components must work together to effectively fulfill the objectives of the Unique Patient Identifier.

GF17. Identifier Components and Operational Characteristics are Critical to the Basic Functions of Unique Patient Identifier

The focus, on the choice of a Unique Patient Identifier, its content/format and assignment, alone will not address the patient identification need. It can neither protect the privacy and confidentiality of patient care information nor assure its accurate identification. These functions depend also on the maintenance of current identification information, security measures such as access security and secure communication, and appropriate technology infrastructure. The six (6) identifier components and operational characteristics provide these capabilities, and in essence give the identifier the necessary functionality.

GF18. Reliable Identification and Confidentiality Require Provider/User Organizations' Participation and Compliance

Although most of the ASTM characteristics such as *assignable, accessible, identifiable,* etc. deal with compliance by the Issuing Authority, healthcare information is created, maintained, accessed and used at healthcare organizations. Positive identification of individuals and access to their patient care information are required at these sites. Therefore, the major threat to the privacy of patient care

information occurs at the user end where the information resides rather than at the issuing end. Appropriate control and security are therefore, required both at the point of issue of Unique Patient Identifier such as a Central Trusted Authority and the point of use, such as a provider organization.

GF19. Check-digits and Encryption are Common to All Options

Check-digit protects against transcription errors and assures accuracy. It can be used to support any numeric identifier. Encryption ensures storage and communication in a secure format. All the Unique Patient Identifier options discussed in this report can make use of this feature. Different encryption schemes yield different encrypted identifier for the same patient. Only authorized users can decrypt the encrypted identifier. Encryption may be used when protection is needed or on a permanent basis. It may be administered either by a Cental Trusted Authority or by provider organizations themselves.

GF20. Development of Technology Infrastructure Requires Direction, Support and Coordination

Alternatives to the Unique Patient Identifier options CORBAMed, HL7 and Directory Service address a critical but only one of the identifier components, namely, the technology infrastructure/software solution. Although these are not identifier initiatives, the selection and industry-wide adoption of a Unique Patient Identifier will help their development and strengthen their capabilities. Basic functions of the Unique Patient Identifier depend on the technology infrastructure.

GF21. Critical Functions are Independent of Identifier Scheme/Value of the Identifier

Critical functions such as access control, identification information, administrative and technology infrastructure, etc. are independent of the numbering scheme or the value of the identifier (i.e. the actual choice of the Unique Patient Identifier). They are not unique or proprietary to any particular Unique Patient Identifier (numbering) scheme or value. They can be implemented with any one of the five Unique Patient Identifier options.

II. Compliance Summary

CS1. All of the Unique Patient Identifier options (SSN, ASTM Sample UHID, LHSTR Number, Personal Immutable Characteristics based Identifier, Bank Card Method and Biometrics) are in general compliance with the ASTM Conceptual Characteristics, with the exception of Biometric method which does not meet 7 of the 30 characteristics.

CS2. Non Unique Patient Identifier options (Medical Record Number, Medical Record Number with Provider Prefix and Cryptography based Identifier) do not meet the ASTM conceptual characteristics adequately.

CS3. Alternatives to Unique Patient Identifier (CORBAMed, HL7, Directory Service, FHOP Standard Data Set and Manual Process) are significantly non

compliant with the ASTM conceptual characteristics.

CS4. Those options that did not comply with the conceptual characteristics, also did not comply with the rest of the requirements including Operational Characteristics, Unique Patient Identifier Component Requirements and Basic Function Requirements.

CS5. Of the five Unique Patient Identifier options that fared well at the conceptual level, Enhanced SSN is the only option that complied with the operational characteristics and component requirements. The remaining four are not operational and they still remain as concepts. In addition, they did not meet the ASTM criteria *"concise"* and only partly met *"usable"*.

CS6. Of these remaining four, Unique the Sample UHID is a well developed concept followed by the LHSTR Number and Personal Immutable Character based Identifier. Even as a concept the Bank Card Method requires significant amount of additional development.

CS7. SSN is used by 20% of the public as Unique Patient Identifier and the SSA is evaluating different options to enhance SSN and fix its current problems.

CS8. A modified Sample UHID is piloted by the Florida VISN as an internal control number (ICN). However, it is used in conjunction with SSN. SSN continues to be the patient identifier (embossed, bar coded and included in the magnetic stripe of their ID card) as the ICN is too long for veterans to remember and users to handle.

CS9. The MRI's proposal, Medical Record Number with Provider Prefix directs the focus away from patient identification to information identification. It designates the Primary Care Physician as the curator to track the previous sites of care for an individual. Therefore, it seems to neglect some of the basic functions of the Unique Patient Identifier.

CS10. Alternatives to Unique Patient Identifier address only one of the components of the Unique Patient Identifier (e.g. technology infrastructure and identification information) CORBAMed, HL7 and Directory Service address the technology infrastructure/software solution and the FHOP option addresses data standardization.

CS11. Options indicate preference for organizations similar to Social Security Administration (SSA) and United States Postal Service (USPS) to address the Administrative Infrastructure component and serve as the Central Trusted Authority. However, the organizational structure, authority, policies and procedures need to be defined and the Infrastructure established. SSA appears to have the most of the processes currently in use.

Available Courses of Action

An Ideal Unique Patient Identifier

Critical functional elements, such as access control, identification information and administrative and technology infrastructures, are independent of the numbering scheme or the value of the identifier (i.e. the actual choice of the Unique Patient Identifier). They are not unique or proprietary to any particular identifier scheme or value. They can be implemented with any one of the five Unique Patient Identifier options. Therefore, a simple user friendly Unique Patient Identifier that is suitable for use by both humans and computers constitutes an ideal choice for the Unique Patient Identifier. In addition, these critical functions are addressed not by the identifier scheme component but by other components. This enables us to separate the identification scheme from all other components. We can, now choose a simple and reliable identification scheme and equip it with all of the required functionality by adding the remaining five components.

Available Courses of Action

Existing options require enhancements to add features/functions and correct existing problems. New options are at a conceptual level and lack operational characteristics and several of the required components. Although none of the options in its present form is a perfect choice, multiple courses of action are available, offering multiple choices. They are:

I. Enhance an existing option

II. Develop a conceptual level option to fruition

III. Develop or facilitate the development of an ideal option.

I. Enhance an Existing Option

The only option that is being currently used as a Unique Patient Identifier is SSN. It is currently used by 20% of the population as a Unique Patient Identifier. It is collected, stored and used as part of patients' demographic information by most of the healthcare organizations. It is also used as a secondary and confirmatory identifier by a large number of provider organizations. With its existing administrative and technology infrastructures and operating procedures, SSN is at a higher level of readiness for use than other options. It meets the conceptual and operational characteristics, and component and basic functions requirements. It is likely to require relatively less time, effort and resources because of its current use and readiness. According to a 1993 Harris poll (Health Information Privacy Survey 1993) the majority of the American population and organizational leaders favor SSN as a patient identifier. It offers an early solution while allowing options that are not fully developed to mature. SSN is a simple, user friendly, Unique Patient Identifier that can be used by both computers and healthcare professionals. Since it is already in use at most of the provider organizations, it is relatively easy to expand its role as the Unique Patient Identifier.

II. Develop a Conceptual Level Option

The remaining options discussed in this report, with the exception of Medical

Record Number, are at a conceptual level. (A modified Sample UHID is piloted as an Internal Control Number to create an MPI and the FHOP Standard Data Set is being tested on patient care data bases to eliminate duplicate records). These options require significant development since they do not already have all of the necessary operational characteristics, Unique Patient Identifier components, administrative or technology infrastructure, implementation plan, policies and operating procedures, etc. A well developed concept such as Sample UHID or LHSTR Number or one of the other options can be chosen based on their ability to meet the ASTM Conceptual Characteristics. It can be developed further to include those characteristics and components that are missing. Implementation of a new choice will avoid any carry over problems and provide a fresh start. But it will require a relatively longer time frame to develop, test and deploy than enhancing and adopting the SSN. Therefore, the impact of time, resource, effort and cost effectiveness must be thoroughly analyzed.

III. Facilitate the Development of an Ideal Solution that Includes all of the Requirements

None of the proposals, including the ASTM Sample UHID, meets all thirty (30) ASTM conceptual characteristics. Most of them are not concise and not suitable for manual calculation and use. Some are not content-free. All are at a conceptual level; some of them with their concept not fully developed.

1) Therefore, instead of limiting the industry to one of these options, an ideal Unique Patient Identifier can rather be developed by consolidating all of the required characteristics. The time frame for its implementation will be comparable to that of implementing one of the proposed conceptual level Unique Patient Identifiers. This course of action will yield the best possible Unique Patient Identifier choice.

2) Alternatively, instead of integrating the independent proposals together, we can foster the independent growth and maturity of the various options. This course of action will provide an opportunity for the competing options to mature. It can be accomplished by establishing leadership, setting the direction and functioning as a catalyst and facilitator to support and promote the growth and development of the various options. Over a period of time, the industry initiatives will mature and multiple efforts converge. Their capability and suitability can be assessed at appropriate intervals, taking into account the passage of the Privacy, Confidentiality and Security legislation by the U.S. Congress. There is an inherent risk that the progress of the options may remain stagnant. Appropriate leadership and support can bring success and benefit to this option. This course of action may cause delay and postpone the implementation of the urgently needed Unique Patient Identifier.

The Need for Leadership

The new options for the Unique Patient Identifier are at a conceptual level. For the new proposals to progress and materialize, a strong leadership is immediately required to steer the process in the right direction. Waiting for the various options to mature and succeed by themselves, may not fulfill the need adequately or in a timely

manner. On the other hand, existing options such as SSN will require the implementation of several enhancements proposed. Therefore, in both cases, a strong leadership with a clear vision is required to steer the process to a successful completion. It will help establish the necessary administrative and technology infrastructures and coordinate the current development processes to progress in harmony to yield the best solution for the Unique Patient Identifier.

Part Two: Patient Identifier

Introduction

U.S. healthcare industry is undergoing a dynamic transformation. The demand for high quality care, increased productivity, cost effectiveness and continuous quality enhancement has triggered rapid restructuring of the healthcare delivery system. This trend, as reflected in managed care and in various integrated delivery systems, has resulted in geographically dispersed and functionally diverse entities such as group practices, independent practice associations, management service organizations, physician/hospital organizations, provider-based organizations, etc. Modern innovations and advances in computer and communication technologies support and foster this transformation to continue into the future. Unique Health Identifiers help to uniquely identify individuals, employers, health plans and healthcare providers within the healthcare system. They establish a comprehensive framework to facilitate exchange of information, access to healthcare, continuity of care, evaluation of quality improvement, outcome measurements and population-based healthcare.

Information technology has changed the way medical record information is stored and retrieved. Computer-based Patient Records (CPRs) have the unique potential to improve the care and well-being of both the individual and the population as a whole. They link an individual's clinical records created by different providers, sites of care and episodes. Computer and communication technologies enable the aggregation of information from CPRs across organizational boundaries to facilitate population-based research, planning and improvement. In order to facilitate the linkage of various clinical records from different care settings and times, and across institutional boundaries, healthcare organizations and computer systems, a valid and reliable patient identification method is required. An identifier that uniquely identifies an individual is a Unique Patient Identifier (UPI). It is required to manage the various clinical and administrative functions relating to the delivery of care.

Several options have been suggested to address the identification requirements of an individual. The objective of this study is to analyze the suitability and efficiency of the various Unique Patient Identifier options. In order to evaluate all functional and operational aspects of these options, this analysis utilizes a two step process. In the first step, various issues surrounding the Unique Patient Identifier, including its required characteristics, capabilities, components, functions and uses, are carefully examined and analyzed. In the next step, the available Unique Patient Identifier options are analyzed in detail for their suitability and efficiency. The report is divided into nine (9) parts:

Part I Executive Summary
Part II Patient Identifier
Part III Unique Patient Identifier (UPI) and Components Integral to UPI
Part IV Privacy, Confidentiality and Security issues relating to UPI

Part V Method of Analysis
Part VI Unique Patient Identifier Options and Alternatives
Part VII Analysis of the UPI Options
Part VIII Central Trusted Authority Options
Part IX Findings and Summary of the Analysis
Part X Available Courses of Action

Patient Identifier - An Integral Part of the Delivery of Patient Care

Healthcare is a multi-disciplinary process. Patient Identifier is used to communicate with members of the multi-disciplinary services and coordinate the delivery of care. During the course of active treatment, the identifier is used for ordering tests, procedures, medication, diet, x-ray, etc. and reporting their results and progress. Other services, such as patient registration, transportation, dietary, scheduling, eligibility verification, billing, coordination of benefits and reimbursement also require the use of a patient identifier. The patient identifier is used to support care during the current encounter as well as retrieve and review the treatment procedures, diagnosis and medications that were provided in the past. Secondary users of healthcare information such as private insurers, health maintenance organizations, federal health agencies and employers depend on Patient Identifiers to perform their business and administrative functions. In short, the patient identifier is an integral part of the delivery of care and health maintenance.

Patient Identifier - A Critical Component of Patient Care Information and Management

Patient Identifier is an integral part of patient care information. It is an essential component in the management of healthcare information and manual record keeping. Key functions such as documentation, manual record keeping, automated collection and storage of information, and access to and communication of information require the use of a patient identifier. Access to historical patient care information (e.g. persistent medical problems, allergy, medication, surgery, etc.) across time is essential for the delivery and continuum of care across multiple providers. Healthcare provider organizations depend on patient identifiers for medical record chart analysis and completion, transcription, chart assembly, coding and abstracting, billing, reimbursement, etc. The Joint Commission on Accreditation of Healthcare Organization's (JCAHO's) Information Management (IM) Standards mandate that the patient identification information be part of a patient's medical record.

Typical Uses of Patient Identifier

Patient Identifier is invaluable to facilitate the current and continuum of care across different providers, care settings and time. Typical uses of Patient Identifier include the following five (5) categories:

1. Coordination of Patient Care Services
Interact with other service domains such as laboratory, x-ray, dietary, physical therapy, etc. and communicate orders, results, request for services, supplies, consultation etc.

2. Record Keeping/Information Management
Collect and organize information such as orders, results, procedures, notes, etc. into a manual medical record chart or in an automated electronic medical record for current and future use.

3. Administrative Functions
Handle administrative functions including billing and reimbursement.

4. Storage and Retrieval of Historical Information
Retrieve and review past medical history including problems, diagnosis, procedures, medication, allergy, etc.

5. Aggregation of information from multiple patient information
Collect, aggregate and perform analysis on groups of patients for treatment efficacy, research, statistical reporting and planning.

Current Method of Patient Identification used in Healthcare Organizations

The current method of patient identification consists of the use of a medical record number, issued and maintained by a practitioner or a provider organization. This medical record number is based on a Master Patient Index (MPI). The numbering system used is generally specific to the individual organization, and the numbers are unique only to that organization. Recently, Hospital Information System (HIS) vendors have begun to develop software to facilitate cross reference to MPIs across an enterprise, often known as Enterprise-wide Master Patient Index (EMPI). In addition to a medical record number, some organizations use a patient account number for billing and reimbursement purposes. Patient account numbers are unique to each patient encounter or visit to the provider. V.A. hospitals, Medicare and the Department of Defense use Social Security Number (SSN) to identify patients.

Impact of Information and Communication Technologies on the Patient Identifier

Computer and communication technologies have transformed the way business functions are carried out. Being the most information-intense industry, healthcare is no exception to this transformation. Physicians and other providers of healthcare depend on accurate and timely information. Healthcare is multi-disciplinary; providers generate, process and communicate care-related information continuously.

Various activities including performance of critical procedures, administration of medication, management of therapies, etc. require communication of an enormous amount of care-related information. Therefore, access to information and communication are fundamental functions in the healthcare industry. In addition, patients themselves are mobile. They visit multiple providers and service centers distributed nation-wide and even across the globe. To manage their care, access and communication must be available both within the same provider organization and across multiple provider organizations regardless of their geographic location. The communication innovations and the transformation of manual documentation into a computer-based patient record have made the sharing of patient care information among healthcare providers across organizational and geographical boundaries close to reality. An identifier that can uniquely identify a patient across different providers and times is the next step to achieve this reality.

The Various Levels of Patient Identifier Usage

The scope of use or the domain within which an identifier is implemented or used will determine the level of usage. The scope of use may be within a single organization or an entire enterprise across the nation or beyond. For convenience, they can be divided into the four (4) levels listed below (All five categories of uses described earlier are applicable to all four levels):

Level I (organization-wide use)

At the lowest level, the identifier's scope of use is limited to functions within the provider organization. The current use of patient identifier by most of the healthcare organizations is at this level.

Level II (enterprise-wide use)

At the next level, the identifier's scope of use includes an entire enterprise. The enterprise may include multiple provider organizations providing same or different types of services. The identifier in this case is used to identify an individual and provide enterprise-wide access to his or her medical record/information. The patient has access to care across the enterprise at this level.

Level III (nation-wide use)

At this level, the identifier's scope is expanded for nation-wide use among healthcare organizations. The full potential of a patient identifier can be realized at this level: 1) access to and use of patient care information from different providers for the purpose of delivery of care, 2) electronic integration of information from different providers, 3) lifelong view of a patient's information and 4) aggregation of population-based information for research and development. The national healthcare reform initiatives, such as managed care and integrated delivery networks, have expanded the patient identifier's scope to a nation-wide use.

Level IV (global-use)

At this level, the identifier's scope is further expanded to world-wide use. All benefits and uses discussed earlier are transformed to global level.

Part Three: Unique Patient Identifier

Unique Patient Identifier

Access to geographically-distributed information requires the patient identifier to expand beyond an institutional level. Existing institution-based medical record numbers are adequate to manage patient identification only within that institution. A robust identification method that can identify individuals uniquely across the nation is essential. The entire healthcare industry including patients, providers and regulatory bodies will benefit from the development and application of a Unique Patient Identifier. Information and communication technologies needed to develop and use such an identifier are currently available.

Industry Initiatives

The need for Unique Patient Identifiers has become urgent and critical. The widespread implementation of information technology and the emergence of computer-based patient records have paved the way for its potential success. Several organizations started to address this issue of Unique Patient Identifier since the beginning of this decade. In 1993, the Computer-based Patient Record Institute created a work group to address the need for a Unique Patient Identifier. Several organizations such as WEDI, AMIA and ACMI called for action in this area by publishing position papers. In 1995, American Society for Testing and Materials (ASTM) published a Standards Guide for the Properties of a Unique Patient Identifier called Universal Health Identifier (UHID). Other organizations such as American National Standards Institute - Healthcare Informatics Standards Planning Panel (ANSI-HISPP), HCFA, HIBCC and NABP worked on identifiers relating to providers, employers, health plans, payer, etc. In 1994, ANSI-HISPP created a task group to review the various options in this area. The recent legislation, Health Insurance Portability and Accountability Act (HIPAA) 1996, requires the implementation of health data standards including identifier standards.

The need for a Unique Patient Identifier and its potential benefits have been recognized widely. Twelve (12) state governments have initiated steps to address this need and an unknown number of private initiatives have emerged to develop a suitable Unique Patient Identifier methodology. The American Health Information Management Association recommends the use of a Unique Patient Identifier to be included in the core data elements of the MPI. The Core Health Data Elements, published by the National Committee on Vital Health Statistics (NCVHS), also includes the use of a Unique Patient Identifier. Industry-wide initiatives such as MPI workshops, consortia initiatives such as OMG/CORBAMed Patient Identification Service and standards organizations initiatives such as HL7 MPI Medication, etc. highlight both the significance of the need for a Unique Patient Identifier and the industry's endeavors to fulfill it. A total of twelve (13) options have been recommended by various proponents. This report includes an analysis of these options.

The Significance of Unique Patient Identifier

Patient Identifier must be unique to meet the critical patient care objectives, such as access to care and patient information, communication, linkage of lifelong health record, population-based studies and integration of information systems. A patient identifier that is non-unique within the national healthcare system presents significant risks and challenges in the following areas:

a) accessing and integrating information from different providers and their information systems.

b) aggregating and providing a lifelong view of a patient's health information

c) supporting population-based research and development

d) cost effectiveness

e) timely access to critical patient care information

f) protecting the privacy and confidentiality of patient information

g) timely delivery of care

h) fraud and abuse, etc.

Currently, the JCAHO Information Management Standards require the following:

1) continuity of care among multiple providers and times (IM#.6)
2) inclusion of patient identification information as part of the patient medical record (IM.3 & IM.7.2)
3) positive identification of the patient for patient care functions such as blood transfusion (QC.5.1.5)
4) use of Unique Patient Identifiers (QC.5.1.4).

A patient identifier that is unique across the entire national healthcare system will facilitate an easy implementation, reduce cost and complexity, and assure timely access to information for patient care, administrative and research purposes.

Unique Patient Identifier - Definition

The identity of an individual consists of a set of personal characters by which that individual can be recognized. Identification is the proof of one's identity. Identifier verifies the sameness of one's identity. Patient Identifier is the value assigned to an individual to facilitate positive identification of that individual for healthcare purposes. Unique Patient Identifier is the value permanently assigned to

an individual for identification purposes and is unique across the entire national healthcare system. Unique Patient Identifier is not shared with any other individual.

Unique Patient Identifier - Basic Functions and Objectives

A Unique Patient Identifier has the potential to assure prompt access to healthcare information, timely delivery of care, linkage of lifelong health records of individuals, aggregation of health information for analysis and research.

The four (4) basic functions that a Unique Patient Identifier must support are:

1) Identification of an Individual:

   a) for the purposes of delivery of care (diagnosis, treatment, blood transfusion, medication, etc.)

   b) for administrative functions (e.g. eligibility, reimbursement, billing, payment, etc.)

2) Identification of Information:

   a) Identification and access to patient information for prompt delivery of care during current encounter, coordination of multi-disciplinary patient care services and communication of orders, results, supplies, etc.

   b) Organization of patient care information into a manual medical record chart or an automated electronic medical record for both current and future use

   c) Manual and automated linkage of various clinical records pertaining to a patient from different practitioners, sites of care and times to form a lifelong view of the patient's record and facilitate the continuity of care in future

   d) Aggregation of information across institutional boundaries for population-based research and planning

3) Accurate identification functions (to provide timely access to patient care information) and dis-identification functions (to support the protection of security, privacy and confidentiality of patient information)

4) Reduce healthcare operational cost and enhance the health status of the nation by supporting both automated and manual patient record management, access to care and information sharing.

Identification of Individuals

Positive Identification for the Delivery of Care

Individual practitioners and provider organizations depend on Unique Patient Identifiers for positive identification of the patient. It is necessary to provide care during the current visit and refer to information from previous visits. Sensitive procedures such as blood transfusion, invasive testing, surgical procedures, medication administration, etc. require positive identification of the patient to prevent mistakes and is mandated by regulatory requirements.

Positive Identification for Administrative Functions

Individual practitioners, provider organizations and other secondary users of healthcare information such as private insurers, health maintenance organizations, federal health plan agencies and employers depend on Unique Patient Identifiers for positive identification (ID) of the patient for verification of eligibility, billing and reimbursement, etc.

Identification of Information

Access to Patient Information and Coordination of Multi-disciplinary Functions

Healthcare is a multi-disciplinary process. Unique Patient Identifier is used to communicate with the members of the multi-disciplinary services. For example, the identifier is used for activities such as ordering of procedures, medications, laboratory tests and radiology examinations, as well as for obtaining and communicating results of tests, procedures and examinations.

Organization of Information & Record Keeping

Both the manual record keeping and automated collection, storage and retrieval of information use Unique Patient Identifier. Medical record keeping functions such as medical record chart assembly, chart analysis, chart completion, medical record abstracting, etc. require the use of a Unique Patient Identifier. Data entry, electronic file organization and retrieval also require a Unique Patient Identifier.

Manual and Automatic Linkage of Lifelong Health Records

The primary focus of healthcare is shifting from treatment of diseases to disease prevention and promotion of health and wellness through consumer education. The health information will cover the entire life span of an individual. The health record of an individual may begin with genetic and prenatal data and end with that individual's death. Therefore, the Unique Patient Identifier can be used to:

a) organize information and documents within a single visit or episode of care,
b) organize information and documents within the same provider organization and
c) identify, organize and link information for the entire life of the individual across multiple providers, institutions and episodes of care.

Both manual charts/files and electronic health information require such an identifier for their creation, maintenance and use.

Aggregate Health Information for Analysis and Research

Practitioners, payers, researchers, policy makers, managers of health systems and care takers of public health need to aggregate health information on the basis of

groups of patients, regions, diseases, treatments, outcomes, etc. The Unique Patient Identifier must facilitate such aggregation and linkage of health information for multiple patients across different geographic regions and times.

Support the Privacy, Confidentiality and Security Protection Functions Relating to Patient Care Information

A reliable identifier helps ensure authorized access and assures protection against unauthorized access. The right to anonymous care and the protection of security, privacy and confidentiality of patient information are major concerns in using a Unique Patient Identifier in a computerized environment. Together with the access control mechanism, the Unique Patient Identifier must aid in protecting the confidentiality of patient information and in identifying the perpetrators who violate patient confidentiality.

Cost Reduction and Improved Care through Access to Information

Through improved access to information, the Unique Patient Identifier: a) enables the prompt delivery of care during the current encounter, b) facilitates continuity of care, c) supports quality of care, d) reduces cost of integration and e) promotes optimum use of information technology.

Components & Processes Integral to Unique Patient Identifier

The Unique Patient Identifier must include components that will provide the various functional capabilities discussed in this report earlier. The identification process includes searching MPIs, matching identifiers, verifying identification information, etc. Depending on the identifier's scope and level of use, these search processes may range from a single provider organization to the entire national healthcare system. Therefore, the Unique Patient Identifier should be supported by a robust technical and administrative infrastructure. In essence, the Unique Patient Identifier will require multiple components to work together to perform its functions and fulfill its objectives. The following six (6) components are integral parts of the Unique Patient Identifier:

1. An Identifier (numeric, alphanumeric, etc.) Scheme

2. Identification Information

3. Index

4. Mechanism to hide or encrypt the Identifier

5. Technology infrastructure to search, identify, match, encrypt, etc.

6. Administrative infrastructure including the Central Governing Authority

Identifier

Patient Identifier is frequently a numeric value such as a sequential or a group of random numbers. Options such as Cryptography Based Identifier and Biometric Identifier however, include numeric and non-numeric characters.

A set of Patient Identification (demographic) Information

The Identifier identifies a patient by matching his or her identification information. Reliable matching of the individual with his or her patient care information requires appropriate amount and category of identifying information relating to the individual and his or her patient care information. Such information falls into the following categories:

a. Permanent Data Segment:

This segment contains the name and permanent (unchanging) personal data such as date of birth, place of birth, mother's maiden name, etc.

b. Longitudinal Data Segment:

This segment contains corroborating information that occur over the lifetime of a person such as address, social security number, state driver license number, profession, name of the spouse, etc.

c. Health Service Data Segment:

This information helps to locate and identify the individual's previous health records and includes type of service, provider ID, date of service, etc. The MPI currently used by hospitals includes such information at an organizational level.

For the Unique Patient Identifier to be effective at all levels, all three segments described above must be available.

Index

The index links the Unique Patient Identifier and the identification information of the patient. It serves as the directory of Unique Patient Identifiers. It must be capable of supporting identification functions within an organization, an enterprise and across the entire national healthcare system.

Organizational Master Patient Index (Organizational MPI)

Individual providers and organizations that treat patients maintain, an index of their patients, called Master Patient Index (MPI). It contains the patient identifiers and the patient's identifying personal and demographic information. The MPI maintained by organizations are unique only within the organization. It serves as a directory of patients for ready reference, verification and identification of the patient and patient information.

Enterprise-wide MPI (EMPI)

Managed Care and Integrated Delivery Network are the results of healthcare reform and related initiatives. Such initiatives bring organizations together and require interoperability among them. An enterprise may contain multiple cooperating provider organizations. The enterprise-wide MPI (or EMPI) provides

cross reference to the multiple provider specific MPIs so that a patient's information can be accessed across the enterprise based on the patient's identifier.

Registry MPI (RMPI)/Software Mediation

Registry MPI is a new concept. It is also called the directory of MPIs. RMPI maintains pointers to those MPIs that are external to the enterprise MPI. RMPIs form a framework for facilitating the searching and matching of patients among different providers and multiple enterprises across the nation. Computer software to support the RMPI mediation functions is being planned by organizations such as HL7 and CORBAMed.

Information from Previous episodes of care and different Sites of Care

Organizational MPIs usually contain information relating to a patient's previous visits. Also, information on previous episodes of care from another organization, but within the same enterprise, can be obtained with the use of the EMPI. However, to access records or information from previous episodes of care from an unrelated organization, the respective site information is essential. Sites external to the enterprise will not be available from the EMPI. Although a RMPI can facilitate searching for a match among cooperating MPIs, sites unknown to a RMPI cannot be accessed for the search.

Protection of Patient Identity (Encryption)

Protection of the identity of a patient can be accomplished with the use of technology such as encryption. Encryption provides protection to patient identifiers when such protection is needed. For example, when communicating sensitive information such as HIV tests or other similar information, the identity of the patient must be protected. Different encryption schemes will yield different encrypted identifiers for the same patient. Only authorized users will be able to decrypt such encrypted identifiers.

Technology Infrastructure

In order to issue, maintain and manage the Unique Patient Identifier, a robust technology infrastructure that includes computer systems, communication network and powerful software applications is required. Such technology will help issue nationwide identifiers, handle encryption and decryption schemes and maintain the data base of identifiers and information relating identifiers.

UPI Communication/Network & Computer Hardware

Unique Patient Identifier has a nation-wide scope. In the future, it can expand to a worldwide use. Therefore, appropriate communication protocols and methodology must be utilized and the operation must be supported by sophisticated and powerful computer and communication networks.

UPI Software Solutions

The Unique Patient Identifier technology infrastructure should include software

applications and communication capabilities that are necessary to perform identification functions, matching patient information and verification of identifiers. Such a computer network must provide nationwide-access twenty four (24) hours a day, 7 days a week and 365 days a year.

Administrative Infrastructure

An administrative infrastructure is required to manage and control the various functions relating to the issue, use and maintenance of the identifier. These functions include:

1. Issue of the identifier
2. Encryption and decryption of the identifier
3. Linkage between the encrypted identifier and non-encrypted identifier
4. Centralized or distributed data base of patient demographic information
5. Assurance of the uniqueness and integrity of the identifier
6. Resolution of conflicts and problems associated with identifiers

Central Trusted Authority

Lack of a Unique Patient Identifier and of a mechanism to track the previous sites of care for an individual leaves a significant gap in the process of identification of a patient and his or her information from previous treatments. A Central Trusted Authority with appropriate power can help fill this gap. In addition, the integrity of the patient identifier is essential to access the patient information reliably; the identifier and the demographic identification information are both highly confidential. The Central Trusted Authority can address these critical functions effectively. The ASTM Standard Guide for Properties of Universal Health Identifier (UHID) and other current Unique Patient Identifier proposals call for the establishment of a Central Trusted Authority. The Central Trusted Authority can be a government agency, a semi-government entity, or a private organization.

In summary, the need for an EMPI, an RMPI, or the Central Trusted Authority, depends on the level of use of an identifier. For example, if the scope of use of an identifier is limited to within a single provider organization it will not require either an EMPI, an RMPI, or a Central Trusted Authority. Access to patient information among multiple enterprises across the nation will require these components.

Processes Integral to Patient Identification:

The identification process varies depending on the scope of access and the level of use of an identifier. The scope may be limited to a single organization, an enterprise, or multiple enterprises across the nation.

Within a Single Organization

Here, the level of use of the patient identifier is at the lowest level (level I). Manual, as well as automated processes, are already in place. The procedures have been well established and a very good control mechanism is in place. Each provider or provider organization maintains an index of patients who were treated. The index

may be manual or automated. A simple card file may serve as a master index in small organizations, and an automated index may be the choice for a larger organization. The index file usually contains the patient's demographic and identification information such as name, date of birth, address, mother's maiden name, SSN, etc. Smaller organizations may use just the name as the identifier. Large organizations that treat a large number of patients with multiple patients with the same name might choose to use a patient identifier such as a medical record number, unit number, or SSN. The patient identifier is used to quickly look up the index to recognize an individual; the demographic information associated with the patient identifier is used to verify and confirm the identity of the individual and his or her record. A majority of provider organizations uses the medical record number/unit number as the patient identifier. These identifiers are designed to be unique only within the same institution. The numbering system used by healthcare organizations is specific to the individual organization. V.A. hospitals, Medicare and the Department of Defense use Social Security Number (SSN) to identify patients.

Enterprise Wide Access (Multiple Provider Organizations)

In response to the Integrated Delivery Network and Healthcare Reform driven initiatives, HIS vendors have developed software solutions that address EMPI functions. EMPI is also known as Corporate MPI. This software solution provides the mapping of an identifier from one provider organization to another within the same enterprise. Several implementations are underway.

Nation Wide Access (Multiple Provider Organizations)

There are two different approaches to addressing the nation-wide access. The first one involves an MPI look up with the use of a Unique Patient Identifier for a match. The second involves the search of an MPI with a given set of demographic information. This method will utilize a weighting algorithm to help the search. The probability of success increases with the use of increased number of demographic characteristics. Organizations such as HL7 and CORBAMed are pursuing the second approach. In fact, both these approaches are complementary to each other. They can become more effective when used together.

Summary

In summary, a simple look up is all that is needed to identify and locate a patient or patient information under a patient identification system designed for use within a single provider organization. An enterprise with multiple provider organizations will require the use of an EMPI, which maps patient identifiers from one organization to another within the enterprise. Patient identification across the entire national healthcare system however, will require additional components and processes such as 1) UPI, 2) RMPI, 3) Central Trusted Authority and 4) powerful and sophisticated computer software for searching, matching and identifying patients.

Part Four: Privacy, Confidentiality & Security

Privacy, Confidentiality and Security of Patient Care Information

Privacy in the healthcare context amounts to the freedom and ability to share an individual's personal and health information in confidence. Confidentiality is the actual protection such information receives from the provider organizations. An individual's personal and health information include those that were supplied by the individual and those observed by the care giver during the course of the delivery of care. Security is the measure that an organization has employed to protect the confidentiality of the patient information. In essence, privacy of an individual's health information depends on the level of confidentiality maintained by organizations, which in turn depends on the security measures implemented by them. Respect for privacy and confidentiality of patient information must be adopted and fostered as an essential organizational policy and culture. Security measures that are failsafe must be utilized. Yet, the organizational security measures can work only within the walls of the organization and among its employees. Protection outside the provider organization requires federal legislative measures, in addition to an organization's security measures. Therefore, protecting the privacy of patient information is a joint responsibility of individuals, organizations and the nation as a whole; appropriate effort must be put forth by all of them.

Unique Patient Identifier's Role in Protecting the Privacy of Patient Care Information

Patient Identifiers play a vital role in the management of patient care delivery and the patient care information. They are also essential for the protection of patient care information. Access to patient care information is managed through the use of the patient identifier. Therefore, Unique Patient Identifiers can assist in the prevention of unauthorized access and accurate identification of the required information. The use of a Unique Patient Identifier to access patient care information helps standardize the access method and strengthens the access control. Unique Patient Identifier eliminates the need for the repetitive use and disclosure of an individual's personal identification information (i.e. name, age, sex, race, marital status, place of residence, etc.) for routine internal and external communications (e.g. orders, results, medication, consultation, etc.) and protects the privacy of the individual. It helps preserve the patient anonymity while facilitating communication and information sharing. Healthcare is fundamentally a multi-disciplinary process. A Unique Patient Identifier enables the integration and the availability of critically needed information from multi-disciplinary sources and multiple care settings. Therefore, the integrity and security of the patient information depend on the use of a reliable Unique Patient Identifier.

Security Risks and the Unique Patient Identifier

One of the risks associated with the use of a Unique Patient Identifier is that it can be misused to link an individual's medical information with his/her personal information such as financial data, purchasing habit, family details, etc. This may result in discrimination (employment, social & financial) and loss of privacy. Since access to healthcare information is possible even without the use of a Unique Patient Identifier, the solution to this and other legitimate concerns does not lie in eliminating the use of a Unique Patient Identifier. The primary mission of the industry is healthcare delivery. The privacy and confidentiality concerns must be addressed fully and effectively; but it should be done without sacrificing any of the required basic components of patient care. Critical needs of timely patient care (such as accurate identification of the patient information and timely access) should not be jeopardized. The risk associated with the use of a Unique Patient Identifier rather sheds light on the overall lack of a public policy relating to the patient care information. The NRC report, For the Record Protecting Electronic Health Information, observes, "Unscrupulous people could of course, collect, collate, and use such data in ways that are prohibited, but the threat of a well-defined and rigorously enforced legal sanctions would help limit such abuses." Therefore, a uniform federal and state legislation is required to protect against misuse of Unique Patient Identifiers, unauthorized access and illegal linkages. Since, Unique Patient Identifier is an integral part of patient care information, it requires the same security and confidentiality protection as the patient care information itself.

The Privacy and Confidentiality Challenge

How do we link patient record, yet mitigate privacy concerns? How do we associate patient information accurately with the proper patient record, yet protect patient anonymity? How can we maximize the benefit of UPI and eliminate risks? Some of the alternatives to Unique Patient Identifier include the use of patient demographic information for indexing, searching and matching. This will subject the patient information to greater privacy risks. Other strategies such as the use of multiple identifiers for the same patients (within the same institution among multiple services or among multiple institutions) will make it difficult for legitimate access to information and subject patient care to undue risks. Some of those who are concerned with the privacy and security risks recommend these alternative methods to prevent unauthorized access. However, computer systems and communication technology are rapidly becoming so powerful and sophisticated that these methods will not be adequate as barriers to prevent unauthorized access. Use of non-standard methods of access to patient care information will increase the level of exposure. Provider organizations will find it difficult to monitor and exercise control over such methods.

On the other hand, the Unique Patient Identifier has the potential to effectively satisfy both of these critical functions (i.e. prevent unauthorized access and perform identification functions). Use of a Unique Patient Identifier to access patient care information helps standardize the access method and enable the organizations to use

a single point of access and solidify their access control. They can monitor the access and continuously improve and strengthen the access control with appropriate measures such as authentication, audit trails, etc. This in turn will ensure timely access to authorized users and better enforcement of security against unauthorized users. The Unique Patient Identifier accomplishes this both within the same organization and across the entire nation. Therefore, the steps required to overcome the privacy and confidentiality challenges are:

1) a judicious design of the identifier
2) organizational security measures to control access
3) uniform federal legislation
4) developing security procedures and instilling responsibility among individuals.

1. Judicious Design

How can we design an identification system that can both fulfill the patient care need and protect the privacy and confidentiality of the patient information? Answer to this most difficult challenge consists of the following design approaches:

1. Separate identification from access
2. Limit the Identifier's capability and use it for identification alone (and not to provide access to the content of patient information).
3. Design the Identifier to be unique
4. Utilize a standard/uniform set of identification information
5. Design Access Control to include
    a) authentication
    b) access privilege
    c) audit trails
    d) separate access to ID segment and patient care information
6. Provide the option to store Unique Patient Identifier in an encrypted format
7. Support the option to communicate it in an encrypted format.

Such a design architecture will keep the identification of patient care information and access as two distinct and separate functions within healthcare. The identifier's role is limited merely to identify the patient record by accessing only the identification segment of patient record and not its content. The access to the patient record, including the identification segment will be handled by the access control function. Both functions are exclusive and mandatory. Policies and procedures to deal with the behavior of individuals and technical measures to protect the data from unauthorized access are functions of the access mechanism and not that of the identifier. Access control will deal with authentication, user identification, access privileges, authorization by way of passwords, audit trails, physical security, etc. This will enable the identification function and security access to complement and support each other by performing exclusively their own distinct roles rather than

assuming each other's.

2. Organizational Security Measures

The following are examples of measures that can be implemented by organizations that generate, access and use patient care information:

1. Access Protection
2. User Authentication
3. Audit Trails
4. Training & Education
5. Physical Security
6. Organizational Policies and Procedures
7. Promoting Organizational Culture that is conducive to the protection of privacy
8. Built in computer hardware & software security:
    a. secure hardware
    b. secure operating systems
    c. secure application software
    d. secure communication protocols and methods

3. Federal Legislation

Federal legislative mandate must:

1. Restrict the use of Unique Patient Identifiers only for healthcare purposes and prevent its use for other purposes

2. Prohibit misuse of patient care information

3. Prohibit discrimination on the basis of patient information

4. Foster the value of privacy relating to healthcare information among public

The Health Insurance Portability and Accountability Act (HIPAA) 1996 requires the U.S. Congress to pass privacy legislation within 36 months. Multiple bills have been introduced for this purpose.

4. Individual Responsibility

Public education of the value of privacy and confidentiality of healthcare information and the legal consequences of violation must be provided nation-wide. Healthcare organizations must provide ongoing staff training to enforce patient's privacy and confidentiality and promote security awareness among employees.

Part Five: Method of Analysis

Scope and Method of Analysis

In 1995, ASTM published the "Standard Guide for Properties of Universal Healthcare Identifier (UHID)". It covers a set of requirements outlining the properties of UHID. It includes altogether thirty (30) characteristics required of a UHID candidate and a temporary identifier provision for emergency use. These characteristics are used here for the evaluation of the seven (7) Unique Patient Identifier options and the seven (7) alternatives. The ASTM characteristics are included in Appendix-A for ready reference.

Though the ASTM Standard Guide is the first effort to conceptualize a Unique Patient Identifier and define its characteristics, its purpose was limited. According to section 9.1, the purpose of the Guide is limited to the conceptual characterization of a UHID, without any involvement in implementation methodology, cost, or policy decisions. It does not include administrative and technology infrastructures requirements, the content of the identification data base (repository), or the structure of the repository. Therefore, the ability of a candidate identifier to meet ASTM characteristics indicates only an intention to meet them in concept.

In addition, the thirty (30) ASTM conceptual characteristics, such as assignable and accessible, address the identifier's format, content, etc. applicable to the point of issue of the identifier (i.e. by a Central Trusted Authority). Healthcare organizations that use the Unique Patient Identifier need to maintain an accurate and up-to-date data base of patient identification information as well. They must also verify the identity of individuals and their information, and control and facilitate the access to patient care information based on Unique Patient Identifier. Since, the ASTM Guide does not address these operational characteristics, in order to fully evaluate the Unique Patient Identifier options beyond a conceptual level, it is necessary to verify their compliance with both the ASTM Standard Guide and other functional and operational capabilities required in live day-to-day patient care environment. Therefore, this analysis includes evaluation of each option's compliance with the following criteria:

1. ASTM's Conceptual Characteristics

2. Unique Patient Identifier's Operational Characteristics

3. Unique Patient Identifier's Components

4. Unique Patient Identifier's Basic Functional Requirements.

1. ASTM's Conceptual Characteristics

For the sake of convenience the ASTM characteristics are grouped by the six categories listed below:

a. Functional Characteristics

b. Linkage of Lifelong Health Record

c. Patient Confidentiality and Security

d. Compatibility with Standards and Technology

e. Design Characteristics

f. Reduction of Cost and Enhanced Health Status

2. Unique Patient Identifiers' Operational Characteristics

In order to analyze the strengths and weaknesses of each option beyond the conceptual level, the following operational characteristics are used:

a. Currently operational vs a concept

b. Existing infrastructure vs infrastructure not in existence, not addressed not required, etc.

c. Readiness of the required technology

d. Timeliness

e. Adequacy of identification information to support identification functions

3. Unique Patient Identifier's Components

As described earlier, there are six (6) basic components that are integral parts of the Unique Patient Identifier. The identifier itself is one of the six components and the remaining five (5) provide the required functional capabilities, administrative and technology infrastructures, and security protection. The six (6) components are:

a. Identifier (numeric, alphanumeric, etc.) Scheme

b. Identification Information

c. Index

d. Mechanism to protect, mask or encrypt the identifier

e. Technology Infrastructure

f. Administrative Infrastructure.

4. Unique Patient Identifier's Basic Functional Requirements

The following are functional requirements at both conceptual and operational levels needed for a Unique Patient Identifier:

i. Identification of individuals

a. For delivery of care

b. For administrative functions

ii. Identification of information

a. Coordination of multi-disciplinary care processes

b. Organization of patient information and medical record keeping

c. Manual and automated linkage of lifelong health records

d. Aggregation of health information for analysis and research

iii.. Support the protection of privacy, confidentiality & security

a. Access Security

b. Judicious Design

c. Content-free Identifier

d. Mask/Hide/Encrypt/Protect/Disidentify

iv. Improve health status and help reduce cost through enhanced access to information and care.

Part Six: Unique Patient Identifier Options and Alternatives

There are Six (6) options for the Unique Patient Identifier, Three (3) for Non Unique Patient Identifiers and Five (5) as Alternatives to the Unique Patient Identifier.

Unique Patient Identifier Options

The following six (6) are the Unique Patient Identifier options:

1. Enhanced Social Security Number proposed by the Computer-based Patient Record Institute (CPRI).

2. ASTM Sample UHID proposed by Dr. Barry Hieb

3. Patient Identification Number based on bank card methods

4. Model UPI based on Personal Immutable Properties

5. Lifetime Human Service and Treatment Record (LHSTR) Number based on the Birth Certificate

6. Biometric Identification.

Non Unique Patient Identifier Options

The following three (3) are Non Unique Patient Identifiers options:

1) Medical Record Number

2) Medical Record Number with a Provider Prefix

3) Cryptography-based Healthcare Identifier

Alternatives to Unique Patient Identifier

The following five (5) are the Alternatives to Unique Patient Identifiers:

1. Manual Process

2. CORBAMed Person Identification Service

3. HL7 MPI Mediation

4. FHOP's Standard Data Set as Common Patient Identifier

5. Directory Service.

The description of each of these fourteen (14) options, their proponents/authors and Documentation are described in detail in the next section (Part Seven: Analysis of Unique Patient Identifier Options). The analysis itself utilizes a common report template.

Part Seven: Analysis of Unique Patient Identifier Options

The various candidate identifiers, with the exception of the manual process, are analyzed based on the four categories of criteria namely:

1. ASTM's Conceptual Characteristics

2. Unique Patient Identifier's Operational Characteristics

3. Unique Patient Identifier's Components

4. Unique Patient Identifier's Basic Functional Requirements.

Report Template

For the sake of consistency, the following template is used for the analysis of each option:

I. Description of the Option

II. Author/Proponent of the Method and Documentation

III. Compliance with ASTM's Conceptual Characteristics

IV. Compliance with Operational Characteristics

V. Compliance with Unique Patient Identifier Components Requirements

VI. Compliance with Basic Functions Requirements

VII. Strengths and Weaknesses

VIII. Potential Barriers and Challenges to Overcoming the Barriers.

IX. Solutions to the Barriers.

Manual Process

As discussed earlier, patient identifier is an integral part of healthcare. Managing the delivery of care process without a patient identifier is an extremely challenging task for healthcare organizations. The current practice of identifying patients involves the use of an identifier such as the medical record number or SSN. Provider organizations that are considerably small in size with low volume of activities can manage their documentation, record keeping, retrieval and other related activities

without a numbering system or an identification method. However, for large organizations that maintain millions of patient records and access thousands of them on a daily basis, manual process is not suitable. An identifier is vital to their daily operation. These organizations use the MPI, which serves as a directory of identifiers. It includes the individual's name, date of birth, address, etc. The identifier facilitates easy identification and enables the collection, organization, analysis, filing and maintenance of all information including documents and images. These are ongoing functions that take place during the course of delivery of care as well as subsequent to the patient's visits for updates, maintenance and retrieval. This identification method is consistent with the record keeping standards followed by other industries as well. The risk associated with the timeliness of care and cost considerations prohibit large organizations from using the time consuming manual processes.

The remaining thirteen (13) candidate options are analyzed in the pages that follow.

1. Enhanced Social Security Number

I. Description of the Option

In 1993, the computer-based Patient Record Institute (CPRI) recommended that SSN with modifications in the number and its process of issuing, be adopted immediately as a "Universal Patient Identifier". Several other organizations such as AMIA, ACMI, ACS, WEDI, ASC X12, NADHO, etc. have also recommended the use of SSN as a Unique Patient Identifier. In 1996, CPRI released an action plan for implementing an Enhanced SSN. CPRI's recommendations for the Enhanced SSN include :

1) confidentiality and security procedures for issuing Unique Patient Identifier by a "trusted authority"

2) federal legislation to provide uniform protection of the confidentiality of health information

3) federal legislation permitting the use of SSN for healthcare purposes

4) mechanism to handle patients without an SSN

5) uniqueness

6) temporary number for emergencies

7) use of demographic information data base to support identification functions

8) use of check-digit verification to ensure accuracy

9) penalties for breach of confidentiality and explicit constraints regarding linkage of health data

10) encryption

11) authentication to verify the identity of the organization requesting a number

12) clean-up of existing duplication, multiple assignments and other errors

13) change in the format of the number to facilitate capacity

14) public education program on Unique Patient Identifier.

In response to the immigration and welfare reform law passed in 1996, the Social Security Administration (SSA) has submitted a report in September, 1997 to the US Congress on options available for enhancing the Social Security Card. SSA studied different methods for improving the Social Security card application process. SSA's

report includes evaluation of various options to issue a counterfeit-resistant ID card with improved security features and functionality. They include:

1) plastic card

2) card with picture

3) secure bar code stripe

4) optical memory stripe

5) magnetic strip

6) magnetic stripe/picture

7) microprocessor/magnetic stripe/picture.

Cost to the government to implement these options in a 3 or 5 or 10 year time period and issue new cards to the 277 million current card holders will range from $3.9 billion to $9.2 billion.

There are about 1300 Social Security offices in the US. SSNs are assigned centrally at SSA Headquarters in Baltimore, Maryland. Applications are handled in Field Offices and Offices of International Operations. SSN is assigned within 24 hours of processing of the application. It has been pointed out even by critics that with 1300 Social Security Offices, well-trained personnel, detailed standard procedural guidelines and an electronic network in place, the SSN can be used as the patient's identifier on relatively short notice. SSN is a demonstrated success as patient identifier in large systems such as Veterans Administration. A majority of the citizens already has SSNs and it is currently used as a patient identifier for about 20% of the population. Other points frequently mentioned in favor of SSN include 1) SSN is the de facto linkage, 2) it already has broad distribution and widespread use, 3) SSN with check-digit is less expensive to implement than a new identifier, 5) people are used to it, 6) systems are accustomed to handling it, 7) SSA continues to make improvements to SSN, 8) government bears the burden of administering the system, 9) used as Medicare ID and 10) relatively easy to adopt.

The initial Social Security Law was passed in 1935. It was called Social Security Account Number (SSAN). In 1943, President Franklin Roosevelt signed an executive order requiring federal agencies to use the SSN whenever a new record system was to be established. The DOD adopted SSN as a military identifier during World War II, and in 1960 the IRS adopted SSN as the tax payer identification number. When the Medicare legislation was passed in 1960, the government adopted the SSN plus an appended letter as the Medicare identification number. The Privacy Act of 1974 prohibited states from using the SSN for enumeration systems other than by authority of the Congress; however, states that were already using it were allowed to continue. The Tax Reform Act of 1976 authorized the states to use

the SSN for a variety of systems including state and local tax authorities, welfare systems, driver's license systems, department of motor vehicles and systems for tracking delinquent child support parents. The SSN is in widespread use as a personal identifier.

II. Author/Proponent and Documentation

1. SSN is already used as an identifier in both healthcare and other industries.
2. SSN is sponsored by several organizations including CPRI, AMIA, ACM, ACS, WEDI, ASC X12 and NADHO. Formal Documentation, 1300 Social Security Offices, well-trained personnel, detailed standard procedural guidelines and an electronic network are in place.

III. Compliance with ASTM Conceptual Characteristics

a) Functional Characteristics:

***Accessible*:** SSA is accessible throughout the nation with its numerous field offices.

***Assignable*:** SSN is assigned within 24 hours, and the postal delivery takes 7 to 10 days. About 1300 field offices provide adequate capability to handle the assignment regardless of the date or place of request. CPRI's recommendation for the Enhanced SSN include improved procedure to process requests for SSN in real time.

Identifiable: SSA maintains a set of identification information on each individual. The amount of identification information collected and stored by the SSA is currently not sufficient to provide the positive identification of an individual for healthcare functions. The Enhanced SSN proposal recommends a data base of individuals' demographic information to support this.

Verifiable: The inclusion of check-digits in the Enhanced SSN has the potential to support the verification process.

Mergeable: SSN's current operating policies and procedures address this function. Multiple numbers have links and cross-references to increase its capability further.

Splittable: SSN's current operating policies and procedures address this function. Currently, a new number is issued upon request . The Enhanced SSN proposal recommends new procedures for the issue and management of the identifier to handle the unique requirements of the healthcare industry.

b) Linkage of Lifelong Health Record

Linkable: SSN is currently used as the patient identifier in large healthcare systems, such as the VA Hospitals and Department of Defense. SSN is used to support the linkage of health records in both a manual and automated environment.

Mappable: SSN is widely used as a secondary identifier by healthcare organizations. Most of the medical record charts include the SSN as a data item. Therefore, it is possible to map SSN to the existing identifiers. This unique capability can also facilitate the mapping of the same individual's medical record in multiple institutions to increase its capability further.

c) Patient Confidentiality and Security

Content Free: The SSN in its current form includes the location and time of issue information. Enhanced SSN proposal recommends changes to the current format.

Controllable: The necessary administrative and technical infrastructures are in place and can provide the control and security necessary for the encryption and decryption functions being proposed for the Enhanced SSN.

Healthcare Focused: The SSN was not created for the use of healthcare. The proposed Enhanced SSN includes check-digits, encryption, improved procedure for the security and issue of SSN, federal privacy legislation against the unauthorized access and misuse of patient information, and appropriate access control. With these additions, the Enhanced SSN has the potential to address the concerns of the healthcare industry adequately.

Secure: The proposed Enhanced SSN encryption and decryption scheme is intended to aid the access security without compromising an individual's privacy. SSA has the necessary administrative and technical infrastructure in place and has the potential to function as the Trusted Authority to govern the policies relating to the encryption and decryption of the identifier. The Enhanced SSN proposal recommends new procedures for the issue and management of the identifier to handle the unique requirements of the healthcare industry.

Disidentifiable: The proposed encryption scheme for the Enhanced SSN enables hiding the identity of the individual that the SSN identifies.

Public: SSN is used widely. It has the potential for encouraging linkages to individuals' social and financial information which can cause harm to them. To address this potential problem, CPRI's proposal for the Enhanced SSN recommends confidentiality and security measures, federal legislation against the misuse of patient identifiers and discrimination based on health information.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** SSN is not based on a industry standard. It is considered to be the de facto standard for personal identification.

Deployable: SSN is currently used in various computer files and formats. It is compatible with technologies such as scanners, bar code readers, etc. The Enhanced SSN proposal includes new procedures for the issue and management of the

identifier to increase its capability further.

Usable: SSN is used currently both in manual and automated modes. Enhanced SSN proposal does not indicate any inhibition to manual or automated use.

e) Design Characteristics

Unique: Under special situations and upon request, SSA's procedures allow the issue of a new number, for example, to protect the identity of the requesting individual. The CPRI's Enhanced SSN proposal includes check digits, encryption and confidentiality and security procedures for issuing Unique Patient Identifiers by a "trusted authority" to assure its uniqueness. These enhancements have the potential to increase SSN's capabilities further.

Repository-based: The Social Security Administration (SSA) maintains a data base of identification information supported by computer networks. The Enhanced SSN proposal includes a data base of individuals' demographic information to support the requirements of healthcare identification functions.

Atomic: SSN can be used as one atomic data element.

Concise: SSN is concise.

Unambiguous: The current SSN includes only numeric characters. The Enhanced SSN proposal recommends an alphanumeric format. This capability will depend on the specifications and design of the proposed enhancements.

Permanent: Enhanced SSN is a permanent identifier.

Centrally governed: The Enhanced SSN proposal requires legislation to fund and task SSA to add check-digit, modify the process of issuing SSN, etc. SSA is well positioned to function as a Central Authority with its 1300 field offices, extensive computer networks, trained personnel and operating procedures already in place. It has the potential to provide the control and security necessary for the encryption and decryption functions, identification and disidentification functions, check-digit verification and other support functions. The proposed enhancements have the potential to increase its repository capability and strengthen the integrity of its identification system as a whole.

Networked: There are about 1300 nation-wide SSA offices with the necessary computer network links already in place.

Longevity**:** CPRI's Enhanced SSN proposal addresses the SSN's lack of capacity to cover the population for a foreseeable future.

Retroactive: Enhanced SSN is aimed at issuing identifiers to all existing individuals.

Universal: CPRI's Enhanced SSN proposal addresses the SSN's lack of capacity to cover the population for a foreseeable future.

Incremental Implementation: SSN is used as a patient identifier by 20% of the population. Most of the medical records in healthcare organizations already use SSN as a secondary identifier. Therefore, this provides a basis for parallel use and incremental implementation of the Enhanced SSN by healthcare organizations.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: SSN is viewed by many as the most realistic option. Its administrative and technology infrastructures are already in place. With implementation of the recommended enhancements such as check-digits, encryption schemes, increased security and improved issuing procedure, Enhanced SSN is likely to be less expensive than other options. It has the potential to function as a Unique Patient Identifier and enhance the health status of the nation through efficient record keeping, sharing of information, reduced cost of integration and optimum use of technology.

IV Compliance with Operational Characteristics and Readiness

Currently operational: SSN is currently operational. It is used as a Unique Patient Identifier in healthcare for about 20% of the population and as a secondary patient identifier by most of the healthcare organizations. It is used in VA hospitals, Department of Defense and Medicare.

Existing infrastructure: SSA is well positioned to function as a Central Authority with its 1300 field offices, extensive computer networks, trained personnel and operating procedures already in place.

Readiness of the required technology: SSN is currently operational. The necessary encryption technology and check-digit methodologies are ready and available for implementing the proposed enhancements.

Timeliness: With the administrative and technology infrastructures and policies and procedures that are in place, Enhanced SSN can be implemented in the shortest time frame.

Adequacy of information to support identification functions: The Enhanced SSN proposal includes the use of a patient's demographic information for supporting the identification functions. In order to link information from previous episodes and different sites of care, record locations and provider information would be needed.

V. Compliance with Unique Patient Identifier

Components Requirements

Identifier: The current SSN has the XXX-XX-XXXX format. The Enhanced SSN proposal includes the addition of alphanumeric characters to increase capacity, and check-digit verification to improve accuracy.

Identification Information: The Enhanced SSN proposal includes the use of a patient's demographic information for supporting the identification functions. In order to link information from previous episodes and different sites of care, record locations and provider information must be addressed by the proposal.

Index: SSA maintains a nation-wide data base of individual's identification information indexed by their SSN.

Mechanism to protect, mask or encrypt the identifier: The Enhanced SSN proposal includes encryption to hide the identifier.

Technology Infrastructure: SSA has a nation-wide technology infrastructure and computer networks to administer the issue and maintenance of the SSN.

Administrative Infrastructure: SSA has 1300 field offices, trained personnel and operating procedures currently in place.

VI. Compliance with Basic Functions Criteria

Compliance with the basic functions criteria depends on compliance with operational characteristics and the identifier component requirements. SSN is in compliance with both of these requirements.

Identification of individuals

Delivery of care functions: Enhanced SSN can support manual and automated verification of the positive identification of an individual required for the active treatment procedures. VA Hospitals and the Department of Defense are currently using SSN for these purposes.

Administrative functions: Enhanced SSN can support the identification functions required of practitioners, provider organizations and secondary users such as insurers, HMOs, federal health plan agencies, etc. for administrative purposes. SSN is currently used by VA Hospitals, the Department of Defense and others for these purposes.

Identification of information

Coordination of multi-disciplinary care processes: Enhanced SSN can support multi-disciplinary functions and coordination of care processes including ordering of procedures, medications and tests, communication of results and consultations. These functions are currently supported by SSN in organizations such as VA Hospitals and the Department of Defense Medical Centers.

Organization of patient information and medical record keeping: Enhanced SSN can support manual medical record keeping and automated collection, storage and retrieval of information. VA Hospitals and the Department of Defense are currently using SSN for these purposes.

Manual and automated linkage of lifelong health records: Enhanced SSN can be used to identify, organize and link information and records across multiple episodes and sites of care. VA Hospitals and the Department of Defense are currently using SSN for these purposes.

Aggregation of health information for analysis and research: Enhanced SSN can support the aggregation of health information on groups of patients, regions, diseases, treatments, outcomes, etc. for research, planning and preventive measures.

Support the protection of privacy, confidentiality & security

Access security: Enhanced SSN recommends access security and authentication procedures for the use of SSN and the protection of patient care information. It can facilitate patient identification without granting access to the patient care information.

Content-free Identifier: SSN in its current format has its location and time of issue. Enhanced SSN proposal recommends changes to both the content and format of SSN to improve security and capacity.

Mask/Hide/Encrypt/Protect/Disidentify: Enhanced SSN proposal includes encryption to protect the Identifier.

Improve health status and help reduce cost

Enhanced SSN currently has administrative and technology infrastructures in place. With implementation of the recommended enhancements, such as check-digits, encryption schemes, increased security and improved issuing procedure, it is likely to be less expensive than other options. It has the potential to function as a Unique Patient Identifier and enhance the health status of the nation through efficient record keeping, sharing of information, reduced cost of integration and optimum use of technology.

VII. Strengths and Weaknesses

Strengths:

1. The Enhanced SSN proposal by CPRI meets:

    a) almost all of the ASTM Conceptual Characteristics (of the 30 requirements, fully meets 27 and partly meets 1),

    b) all of the Operational Characteristics,

    c) Unique Patient Identifier Component requirements and

d) Basic Functions Criteria.

2. The Enhanced SSN's strength also includes:

a) Existing infrastructure

b) Trained Staff

c) Policies, procedures and guidelines in place

d) Ongoing improvements by the SSA

3. CPRI has identified SSN's limitations due to its current structured format and the potential for problems due to its widespread use and provided recommendations to eliminate them. Proposed enhancements to eliminate deficiencies and improve capabilities include:

a) encryption scheme
b) addition of check-digits
c) improvement to issuing procedures
d) clean-up of existing duplications, multiple assignments and other errors.
d) confidentiality and security measures
e) legislation to prevent misuse and discrimination
f) mechanism to handle patients without SSN
g) temporary ID for emergency use
h) change in the format to facilitate capacity

4. Several approaches described in the ASTM Guide including the encryption scheme can be used in conjunction with the Enhanced SSN to yield the same benefit as a UHID (e.g. multiple Encrypted IDs with links to the Enhanced SSN).
5. Already used by 20% of the public
6. Least expensive to implement
7. Relatively easy to adopt - people are used to it and systems are accustomed to handling it.
8. Speed of implementation
9. According to Harris poll, the majority of the American population and organizational leaders favor SSN as a patient identifier

Weaknesses:

The weakness relates mainly to those SSN's problems already being addressed in the CPRI's Enhanced SSN proposal. They are:

1. Incomplete and delayed issue of SSN at birth (Enumeration at Birth):

Connecticut, Rhode Island, Oklahoma, Alaska and California are not participating in the current "Enumeration at Birth" program

2. Typical time required to obtain a SSN is measured in weeks rather than "minutes" required by healthcare

3. No provision for the use of temporary numbers

4. Error level: significant percentage of error level exists in SSNs

5. Check digits: The SSN system was designed before the computer era. Therefore, no provision such as check-digits was made to check the errors

6. No mechanism to use the SSN in a non-identifiable manner

7. Not healthcare focused - control of the SSN is vested in organizations which are not driven by the needs of health care

8. About 10 million individuals in the U.S. do not have the SSN. Illegal aliens and visitors do not possess SSN. Illegal aliens, without SSN, seeking delayed care due to fear, can increase healthcare cost.

9. SSN does not have exit control (upon death or permanently leaving the country)

10. SSN lacks flexibility due to the block structure (XXX-XX-XXXX). It does not have sufficient digits to handle the identification need for a foreseeable future.

11. There are often multiple holders of the same SSN (less well-informed immigrant households). About 4 million individuals are estimated to have multiple SSNs.

12. Lacks ability to provide retroactive legal protection (SSN too widely used already).

13. The SSN is in extraordinarily wide use as a personal identifier. It has the potential for linkage with non-healthcare data bases.

14. The allowable entries in each of the three groups in an SSN are well known. Therefore, it is easy to counterfeit an SSN.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

In summary, the barriers relating to SSN fall under the three major categories listed below:

1) Inadequate administration for healthcare purposes, i.e. existing error level,

incomplete issue, lack of mechanism for emergency issue, lack of check digit and capacity for future growth.

2) Privacy and confidentiality risks due to SSN's use in non-healthcare areas in the absence of legislation and legal protection.

3) Cost, length of time and complexity involved in correcting and enhancing SSN problems.

4) Enactment of the necessary federal legislation (both privacy legislation and legislation permitting SSN's use in healthcare).

IX. Solutions to the Barriers:

1. Elimination of errors, duplicate numbers and multiple SSNs that already exist in the system

2. Access control and prevention of misuse via adequate federal legislation for 1) protection of individual's privacy, 2) confidentiality of health information and 3) protection against social and financial harm

3. Self check-digit to prevent transcription errors

4. Encryption and Decryption Scheme to protect the privacy of the identifier

5. Use of temporary numbers for emergencies

6. Improved procedure for assigning SSNs to accommodate infants and others who would not ordinarily be assigned SSN.

The Enhanced SSN proposal includes these solutions. Upon implementation, they have the potential to effectively overcome the barriers and eliminate the weaknesses listed above.

2. Sample Universal Healthcare Identifier (UHID)

I. Description of the Option

ASTM's "Standard Guide for Properties of a Universal Healthcare Identifier (UHID)" deals with the conceptual characterization of a UHID. It defines thirty (30) characteristics required of a UHID. The scope of the guide does not include implementation methodology, cost, or policy decisions. Encrypted UHIDs (EUHIDs) are included in the guide for hiding the identity of individuals while linking information. Separate EUHIDs are allowed for different episodes of care for the same patient. The guide also recommends the use of temporary patient identifiers (TPIs) controlled by individual organizations for emergency use and requires them to subsequently transfer all information to the correct UHID.

The UHID requires a Central Trusted Authority for processing request for a UHID. The Central Trusted Authority's responsibility will include issuing the sequential UHID, computing the check-digit, choosing the encryption scheme, generating the EUHID and maintaining either a cross index between UHID and EUHID or an appropriate decryption scheme to link the UHID and the corresponding EUHID. Therefore, the implementation of UHID will depend on the establishment of a Central Trusted Authority.

1. UHID Sample

The guide provides a sample UHID and illustrates the application of the 30 UHID criteria to evaluate candidate UHIDs. The sample UHID and the illustration are not part of the ASTM Standards. The sample UHID consists of a sixteen (16) digit sequential identifier, a "." (period) that serves as a delimiter, a six (6) digit check-digit and a six (6) digit encryption scheme. Altogether, it consists of 28 numeric digits and a period. Dr. Barry Hieb, M.D. of Sunquest, Inc. proposes the sample UHID which was provided in the ASTM guide solely for the purpose of illustration for a candidate Unique Patient Identifier.

2. Internal Control Number (ICN) based on ASTM Guide

The Veterans Integrated Systems Network (VISN) in Florida is piloting the development and use of an Internal Control Number (ICN) based on the ASTM guide. The ICN is used for cross-indexing patients that visit multiple sites of care. The Veterans Health Administration (VHA) System maintains a national data base of patients' visit information received from the various VHA medical centers. The ICN works in conjunction with the national data base to track the locations of a patient's record. It uses patient identifiers and record locations to accomplish the cross indexing. VHA's objective is to create an index of ICNs (Master Patient Index) that uniquely ties the distributed records to patients. The ICN Master Patient Index includes patient identifier(s) and record locations. Mismatch and discrepancies are reported to respective sites and resolved with human intervention. ICN structure model does not include the trusted authority or the use of EUHID. Currently, the

sample UHID is being piloted at three sites (Tampa, Gainesville and Lake City).

In November of 1996, the U. S. Department of Veterans Affairs (VA) issued its new Veterans Universal Access Identification Card with SSN, patient's photo and date of birth. The new card has these information printed, embossed, bar coded and also included in its magnetic stripe. It is used to identify patients and retrieve their demographic information during the course of active treatment. To handle patient encounters, SSN continues to be VHA's system-wide patient identifier. The ICN is piloted to serve as an internal control number to build a system wide Master Patient Index for cross referencing the distributed patient information.

II. Author/Proponent and Documentation

1. The ASTM's E 1714 - 95 "Standard Guide for Properties of a Universal Healthcare Identifier (UHID)" and the example outlined in it are the formal documentation for the sample UHID proposed by Dr. Barry Hieb.

2. The ASTM E 1714-95 "Standard Guide for Properties of a Universal Healthcare Identifier (UHID)", by itself is not a proposal for a Unique Patient Identifier

3. The VHA project is the development of an internal control number based on the ASTM guide to reference patient identifiers, locate records across the VHA System and build a Master Patient Index based on the internal control number. It is not a separate proposal for a Unique Patient Identifier.

Therefore, only Dr. Barry Hieb's Sample UHID proposal is analyzed here.

UHID SAMPLE

Both the ASTM guide and the example do not address implementation methodology. ASTM points out in its own evaluation that the sample UHID meets the ASTM criteria in concept, but its ability to meet the criteria in practice will depend on implementation methodology, policies and procedures, and the necessary administrative and technology infrastructure in place (Central Trusted Authority). In order for these components to be in place, planning and extensive preparation is required. It includes the designation of a central trusted authority, funding and development of specifications, design, testing, deployment, etc. The evaluation below is based on information currently available.

III. Compliance with ASTM Conceptual Characteristics

a) Functional Characteristics:

***Accessible*:** Access is dependent upon the establishment of a network infrastructure, the trusted authority and policies and procedures that support the system.

***Assignable*:** Assignment of the Sample UHID or EUHID, regardless of time or place

of request, depends on the establishment and functions of a network infrastructure, the trusted authority, and the implementation of policies and procedures that support the system. It will also depend on the mechanism to request a Sample UHID.

Identifiable: This will depend on the identification information that the trusted authority links to the Sample UHID.

Verifiable: The Sample UHID includes a six (6) digit check-digit for verification.

Mergeable: The internal data structure of the Sample UHID does not directly support merging duplicate or redundant identifiers. They can be linked at the trusted authority.

Splittable: There is no inherent support for splitting the Sample UHID. New IDs can be issued for future use. Splitting for retroactive information must be handled by the trusted authority.

b) Linkage of Lifelong Health Record

Linkable: The Sample UHID has the ability to function as a data element and support the linkage of health records in both manual and automated environment.

Mappable*:* With the use of appropriate database system and software, the Sample UHID can be used to map currently existing healthcare identifiers.

c) Patient Confidentiality and Access Security

Content Free: The Sample UHID is free of information about the individual.

Controllable: This depends on the policies and methods that will be adopted by the trusted authority.

Healthcare Focused: The Sample UHID is recommended solely for the purpose of healthcare application.

Secure: The Sample UHID includes an EUHID which offers mechanism for secure operation through the use of encryption and decryption processes. These capabilities depend on the policies and procedures that will be implemented by the trusted authority.

Disidentifiable: EUHID supports multiple encryption schemes offering multiple EUHIDs to prevent revealing the identification of the individual.

Public: The EUHID's encryption scheme is intended to hide the identity of individual when linking information. However, public disclosure of a patient identifier without any risk to the privacy and confidentiality of patient information depends on appropriate access security and privacy legislation, similar to other

identifiers.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** The Sample UHID is not based on existing industry standards. It is based on ASTM's Standard Guide for Properties of a Universal Healthcare Identifier (UHID).

Deployable: The Sample UHID is capable of implementation in a variety of technologies such as scanners, bar code readers, etc.

Usable: The Sample UHID is capable of implementation in a variety of technologies such as scanners, bar code readers, etc. The 28 digit identifier will present difficulty for manual computation and transcription. It may be a time-consuming process and subject to human errors.

e) Design Characteristics

The ASTM guide and the proposed Sample UHID do not address the implementation issues and infrastructure requirements.

Unique: The trusted authority will be responsible for the uniqueness of the Sample UHID.

Repository-based: The Sample UHID can be stored in a repository.

Atomic: The Sample UHID consists of a sixteen (16) digit sequential identifier, a one (1) character delimiter, a six (6) digit check-digit and a six (6) digit encryption scheme. It can function as a single compound data element.

Concise: The Sample UHID is not concise. It is a 29-character length identifier.

Unambiguous: The Sample UHID is unambiguous. It uses numeric characters and a period as a delimiter.

Permanent: The Sample UHID has sufficient capacity to prevent reuse of identifiers.

Centrally governed: This policy issue is not addressed. The Sample UHID requires central administration and is dependent on the establishment and functions of a trusted authority.

Networked: The Sample UHID can be operated on a computer network. It requires establishment of the necessary network and technology infrastructure.

***Longevity*:** The Sample UHID can support patient identification for a foreseeable future.

Retroactive: Has the capacity for retroactive assignment of the Sample UHID to every person in the United States

Universal: Can support patient identification for the entire world population

Incremental Implementation: The Sample UHID can be implemented on an incremental basis. With the development and use of appropriate procedures and establishment of the necessary bidirectional mapping, both the Sample UHID and existing patient identifiers can co-exist during the time of transition.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: The Sample UHID has the potential to support the functions of a Unique Patient Identifier. The establishment of both the administrative and technology infrastructures, the creation of a Trusted Authority, the design and development of computer software, hardware and communication networks, and the implementation security measures will require substantial investment of resources, time and effort.

IV. Compliance with Operational Characteristics and Readiness

Currently operational: The Sample UHID is not currently operational. The ICN involved in the VHA's Florida pilot project is used as an internal control number for cross indexing records distributed among multiple providers and not as a patient identifier. It does not include encryption (EUHID) and Central Trusted Authority.

Existing infrastructure: Does not have existing administrative or technical infrastructure. The sample UHID relies on the Central Trusted Authority to administer its functions such as encryption, repository, check-digits, uniqueness, security, etc.

Readiness of the required technology: The basic technologies to support encryption and check-digit methodologies are ready and available.

Timeliness: The administrative and technology infrastructures (Central Trusted Authority, software, hardware, communication network, etc.), and the implementation methodology, policies and procedures, must be designed and developed before the Sample UHID's nation-wide implementation. This will require a substantial amount of time.

Adequacy of identification information to support identification functions: A repository is part of the conceptual characteristics, but the Sample UHID does not discuss its content or structure. The record location or provider information necessary to access a patient's medical record distributed among multiple providers is also not addressed.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
The Sample UHID's focus is mainly on the Identifier Component. The 29-character ID format (16 digit sequential ID followed by a six digit check-digit and a six digit encryption scheme and a "." as delimiter) provides ample capacity. The length of the identifier will be difficult for patients to remember and users to process manually.

Identification Information
The Sample UHID requires the use of a patient's identifying data elements such as name, date of birth, sex, etc. But it does not address the content or structure of the data base that will contain such data elements.

Index
The proposal indicates that Sample UHIDs will be stored in a data base and linked with patient's identification information. It does not address the content and use of an index such as a Master Patient Index that can provide this link. It requires a central governing body for administration, but does not indicate whether local, regional, or central MPIs will be used.

Mechanism to protect, mask or encrypt the identifier
Provides a six (6) digit encryption scheme capable of generating multiple encrypted UHID for a single patient.

Technology Infrastructure
Does not have an existing technology infrastructure. The technology infrastructure is not addressed in the proposal.

Administrative Infrastructure
Does not have an existing administrative infrastructure. The Sample UHID requires a Central Trusted Authority, but it does not include a proposal for the administrative infrastructure.

VI Compliance with Basic Functions Criteria

Compliance with the basic functions criteria depends on the identifier's compliance with operational characteristics and the identifier components requirements. The Sample UHID does not meet several of the operational characteristics. It addresses only two of the six Unique Patient Identifier components, namely the identifier component and encryption protection. It treats the remaining four components (Patient Identification Information, Index, Technology Infrastructure and Administrative Infrastructure) as implementation and policy issues, outside the scope of the proposal. However, the identifier and the encryption scheme are dependent on the establishment and implementation of these four components. In the absence of these components and the required operational characteristics, the Sample UHID's ability to fulfill the basic functions discussed below is unknown and uncertain.

UHID's 29-character length is unsuitable for manual calculation/use. Therefore, at best, it can only partially meet the Unique Patient Identifier's basic functions.

Identification of individuals

Delivery of Care Functions: The Sample UHID's ability to support the positive identification of an individual required during the course of active treatment will depend on its ability to address both the implementation of the remaining identifier components and all of the operational requirements. The length of the identifier will not be conducive for patients to remember and for users to process manually.

Administrative Functions: The Sample UHID's ability to support the identification for administrative functions required by practitioners, provider organizations, insurers, HMOs, federal health plan agencies, etc. will depend on its ability to address both the implementation of the remaining identifier components and all of the operational requirements. The length of the identifier will not be conducive to manual use by patients, providers, payers, etc.

Identification of information

Coordination of Multi-disciplinary Care Processes: The Sample UHID's ability to support multi-disciplinary functions and coordination of care processes including, ordering of procedures, medications and tests, communication of results and consultations will depend on its ability to address both the implementation of the remaining identifier components and the operational requirements. The length of the identifier will not be conducive to manual use such as verbal communication, telephone enquiry and personal interactions.

Organization of Patient Information and Medical Record Keeping: The Sample UHID's ability to support manual medical record keeping and automated collection, storage and retrieval of information will depend on its ability to address both the implementation of the remaining identifier components and the operational requirements. The length of the identifier will not be conducive to manual use. Currently, most provider organizations are required to maintain manual medical records in addition to electronic information.

Manual and Automated Linkage of Lifelong Health Records: The Sample UHID's ability to identify, organize and link information and records across multiple episodes and sites of care will depend on its ability to address both the implementation of the remaining identifier components and all of the operational requirements. The length of the identifier will not be conducive to manual use.

Aggregation of Health Information for Analysis and Research: The Sample UHID's ability to support the aggregation of health information on the basis of groups of patients, regions, diseases, treatments, outcomes, etc. for research, planning and preventive measures will depend on its ability to address both the implementation of the remaining identifier components and the operational requirements.

Support the protection of privacy, confidentiality & security

Access Security: The Access Security and the authentication procedures needed to access the patient care information are not addressed.

Content-free Identifier: The Sample UHID is a content-free Identifier.

Mask/Hide/Encrypt/Protect/Disidentify: The Sample UHID proposal includes encryption to protect the Identifier. This capability will depend on its ability to address both the implementation of the remaining identifier components and all of the operational requirements.

Improve health status and help reduce cost

The Sample UHID has the potential to support the functions of a Unique Patient Identifier. It is contingent upon the establishment of both the administrative and technology infrastructures, the creation of a Trusted Authority, the design and development of computer software, hardware and communication networks and the implementation of security measures. According to ASTM's own evaluation the cost of implementing UHID will be substantial. The nation-wide implementation of a new system will require a huge investment of resources, time and effort.

VII. Strengths and Weaknesses

Strengths:

1. Meets almost all of the ASTM conceptual characteristics (of the 30 requirements, fully meets 25 and partly meets 1)

2. The Sample UHID is a new choice with a new start without known defects or limitations.

3. Avoids crossover problems from an existing system that need to be corrected or those that cannot be corrected retrospectively

4. A six (6) digit check-digit to assure high degree of accuracy

5. Encryption scheme that permits multiple EUHIDs to protect the confidentiality of patient information

6. Provides an opportunity to design an identification system that will fully take advantage of existing technology

7. Offers capacity to handle the nation's population for a foreseeable future.

Weaknesses:

1. Does not meet three of five operational characteristics and does not fully address the fourth characteristic

2. Meets only two of the six identifier component requirements

3. Length of the ASTM Sample UHID makes it less user-friendly for manual computation and transcription and is subject to human errors.

4. UHID may be less user-friendly for functions such as current medical record keeping functions, personal interactions, verbal communications and coordination of multi-disciplinary team work, etc.

5. Untested - implementing a brand new system nationwide that has not been tested has inherent risk for its success.

6. Lack of existing infrastructure, plan and procedures - The Sample UHID requires the development of an implementation plan for the establishment of necessary infrastructure including the trusted authority, definition of its power, organizational structure and operating procedures.

7. Significant cost - planning, design, development and implementation of the Sample UHID proposal will require substantial investment of resources, a huge effort and a longer time frame than enhancing an existing identification system.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. Establishment of administrative infrastructure including the Central Trusted Authority

2. Development of policies, procedures and implementation methodologies not addressed in the proposal

3. Inclusion of missing identifier components such as patient's identification information, record locations, provider information and the necessary index

4. Development of technology infrastructure including the software application, communication systems, encryption methodology and control, access security, etc.

5. Enactment of privacy and security legislation

6. Substantial investment of resources, time and effort

7. Timeliness.

IX. Solutions to the Barriers:

1. Immediate establishment of study/implementation teams to work on:

    1. Establishment of administrative infrastructure including the Central Trusted Authority

2. Development of the policies, procedures and implementation methodologies not addressed in the proposal

3. Inclusion of missing identifier components such as patient's identification information, record locations, provider information and the necessary index

4. Development of the necessary technology infrastructure including the software application, communication systems, encryption methodology and control, access security, etc.

5. Enactment of the privacy and security legislation

6. Required investment of resource and effort

7. Timeliness of the solution.

3. Unique Patient Identifier based on Bank Card Method

I. Description of the Option

The bank card/financial card industry has a demonstrated success with its plastic card identification systems. It can be utilized to design and manage the healthcare ID system. The experience, know-how and capability to implement such a system is in the private industry and not in the government. Therefore, the capabilities of the industry must be exploited to develop, implement and manage the operation after transition. The necessary technology such as inexpensive card readers that respond to keystrokes or magnetic-stripe, printers etc. has already been developed. The industry has considerable experience in issuing and replacing (lost) cards. In 1994, Dr. Willis Ware from RAND, the proponent of this method recommended that a comprehensive set of requirements be developed by a team of payers, medical practitioners, hospital administrators, clinical managers, etc., and that competitive RFP sent to the card industry to assume charge of developing, implementing and managing this process during and after transition.

The initial design recommendation of Dr. Willis Ware consisted of a 13 to 15 digit identifier with a set of digits to identify the practitioner or the medical group, another set of digits to identify payers, a third set of digits to identify the individual and finally check digits to control errors. The use of separate additional digits to identify conditions such as allergies, disease, etc. was also suggested. The proposal included a credit card-type plastic card as the identification medium with an authenticator such as mother's maiden name or date of birth "woven" into the card along with the individual's name as a easily read identifier for convenience. Dr. Ware ruled out the use of magnetic stripe due to frequent accidental erasure by refrigerator magnets or large electrical equipment.

Conversation with Dr. Willis Ware during this study, however, indicated significant changes to his original thinking. He preferred the smart card in place of Bank Card as the medium and recommended against the inclusion of any patient care information in the card or the identifier.

II. Author/Proponent and Documentation

1. Bank Card Identification Method has been in use for a long time in the financial services industry for applications, such as banking, credit transactions and travel.

2. The method was recommended by Dr. Willis Ware, RAND Corporation. His past document outlining his original method is the only document available for review.

III. Compliance with ASTM Conceptual Characteristics

The proponent of this method, Dr. Willis Ware, has recommended the following steps for the design and implementation of the Bank Card Method:

1. Organize a team of healthcare providers, payers, medical practitioners, hospital administrators, clinical managers, etc.

2. Develop a comprehensive set of requirements for the design, format and content of the card.

3. Prepare and send a competitive RFP to the card industry to assume charge of developing, implementing and managing this process during and after transition.

Dr. Ware indicated that his current interests and involvement with patient identifier were limited and these steps have not occurred. The current procedure to obtain a Bank Card requires the submission of an application to the financial institution. An individual can have multiple Bank Cards each with a different identification number. Dr. Ware's concept needs to be developed further to fully understand his method, design, characteristics, functions and processes.

a) Functional Characteristics

Accessible: Dr. Ware recommends a Central Trusted Authority or a tightly controlled regional or state authority for the issue and maintenance of the method.

Assignable: The Bank Card Method requires a Central Trusted Authority or a tightly controlled regional or state authority to assign and maintain the identifier.

Identifiable: The issue of identifiers will be based on personal identification information. However, the necessary specifications, design and development are yet to be planned.

Verifiable*:* Check-digit verification is included in the proposal.

Mergeable**:** This can be accomplished at the regional or at the Central Trusted Authority level. However, this capability will be subject to policies, procedures, specifications, design and development that are yet to be planned.

Splittable: This can be addressed with appropriate procedures at the regional or at the Central Trusted Authority level.

b) Linkage of Lifelong Health Record

Linkable: The Unique Patient Identifier based on Bank Card Method can be used to link patient records from multiple sources.

Mappable: Bidirectional linkage is possible between the Unique Patient Identifier based on Bank Card Method and the existing Identifiers.

c) Patient Confidentiality and Security

Content Free: Dr. Ware's current thinking has changed his original proposal with regard to this characteristic. The Bank Card Method is content-free. However, this capability will be subject to the final specifications, design and development that are yet to be planned.

Controllable: The proposal does not include encryption. However, this number can be encrypted and encryption schemes administered by a Central Trusted Authority, or regional/state authority.

Healthcare Focused**:** Dr. Ware's proposal is specific to healthcare.

Secure: The Unique Patient Identifier based on the Bank Card Method can be encrypted and the security administered by the Central Trusted Authority. However, the proposal does not include encryption.

Disidentifiable: The Unique Patient Identifier based on Bank Card Method can be encrypted to protect the identifier.

Public: Public disclosure of the Unique Patient Identifier without risks to privacy and confidentiality of patient information is not discussed. It will depend on appropriate access security and privacy legislation. The patient ID is not intended to be a public information.

d) Compatibility with Standards and Technology

Based on Industry Standards**:** Bank cards that are currently in use are based on industry standard. However, the compatibility with the industry standard for healthcare purpose will depend on the appropriate specification, design and development that are yet to be organized.

Deployable: The Bank Cards are in extensive use. The necessary technology, such as inexpensive card readers that respond to keystrokes or magnetic-stripe, printers etc. has already been developed.

Usable: Bank Card is used in both manual and automated modes.

e) Design Characteristics

Bank Cards are issued by individual banks. The issuing organizations follow common standards with regard to its content and processes. Dr. Willis Ware recommends that the method can be administered either by a Central Trusted Authority or by establishing a tightly controlled regional/state authority.

Unique: The information contained in the magnetic stripe is standardized across the industry. However, the account numbers issued and maintained by individual banks are not unique. An individual can have multiple ID numbers. Therefore, this capability is subject to the development of appropriate specification and design that

are yet to be done.

Repository-based: Banks maintain a data base of identifying information for each individual. They also use authentication processes with data elements such as mother's maiden name, data of birth, etc. Therefore, it is possible to meet this requirement subject to appropriate specifications, design and development that are yet to be done.

Atomic: Although the number includes groups of numbers, it can function as a single data element.

Concise: Bank Card Method Numbers are moderately concise.

Unambiguous: Bank Card Method does not include alphanumeric characters. Therefore, it is unambiguous.

Permanent: The Unique Patient Identifier based on Bank Card Method is a permanent identifier.

Centrally governed: Dr. Willis Ware proposes that this method be administered either by a Central Trusted Authority or by establishing a tightly controlled regional/state authority.

Networked: Telephone, telecommunication (modem) and online links are currently utilized for inquiry with regard to approval and transmission of credit and debit transactions. It can be operated on a network.

Longevity: This option can support patient identification for a foreseeable future.

Retroactive: Bank Card method can be used for retroactive assignment of identifiers.

Universal: This method can support universal use. However, this capability will be subject to specifications, design and development that are yet to be planned.

Incremental Implementation: Can be implemented incrementally.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: This capability is subject to specifications, design and development that are yet to be planned.

IV. Compliance with Operational Characteristics and

Readiness

Currently operational: The Bank Card Method is not currently operational as a Unique Patient Identifier.

Existing infrastructure: Does not have existing administrative and technical infrastructures

Readiness of the required technology: Telephone, online links, modem, card readers, point of sale terminals etc. are currently available and utilized by financial institutions.

Timeliness: The Bank Card Method is not a fully developed concept. It needs to be developed further to address healthcare applications. It is not ready for implementation and requires significant amount of additional time for implementation.

Adequacy of information to support identification functions: The Patient identification data base and its contents have not yet been addressed.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
Dr. Willis Ware's proposal for the Unique Patient Identifier based on Bank Card Method consists of 13 to 15 digits. The Bank Card Method remains as a concept. The identifier format has not been finalized.

Identification Information
The Patient identification data base and its contents have not yet been addressed. The Bank Card Method remains as a concept. It is not ready for implementation.

Index
The index that would link the identifier and the patient's identification information has not been addressed. The Bank Card Method needs to be developed further.

Mechanism to protect, mask or encrypt the identifier
Encryption is not part of the proposal.

Technology Infrastructure
Dr. Ware's proposal requires the use of the card industry to serve as the technology infrastructure. He recommends issuing a competitive RFP to the card industry for the design and implementation of the method, which remains as a concept now.

Administrative Infrastructure
The proposal recommends either a Central Trusted Authority or a tightly controlled regional/state authority which is not in existence at this time.

VI. Compliance with Basic Functions Criteria

Compliance with the basic functions criteria depends on the identifier's compliance with operational characteristics and the required identifier components. The Bank Card Method proposal is at a preliminary stage. Dr. Willis Ware's steps relating to organizing a team of experts, developing specifications and issuing an RFP to the card industry have not taken place. The proposal needs further development before its capabilities can be compared with other options. Currently the method does not meet all of the operational characteristics and component requirements. Therefore, the Bank Card Method's ability to perform all of the basic functions discussed below is unknown. It will depend on the development of a complete proposal and inclusion of missing components and operational requirements.

Identification of individuals

Delivery of care functions: The ability to support the manual and automated identification of an individual will depend on the final format and content of the identifier, implementation of the remaining Unique Patient Identifier components and the capability to address all of the operational requirements.

Administrative functions: The ability to support the identification required by practitioners, provider organizations and secondary users for administrative functions will depend on the final format and content of the identifier, implementation of the remaining Unique Patient Identifier components and the capability to address all of the operational requirements.

Identification of information

Coordination of multi-disciplinary care processes: The ability to support multi-disciplinary functions and coordination of care processes including ordering of procedures, medications and tests, communication of results and consultations will depend on the implementation of the remaining Unique Patient Identifier components and the capability to address all of the operational requirements.

Organization of patient information and medical record keeping: The ability to support manual medical record keeping and automated collection, storage and retrieval of information will depend on the implementation of the remaining Unique Patient Identifier components and the capability to address all of the operational requirements.

Manual and automated linkage of lifelong health records: The ability to identify, organize and link information and records across multiple episodes of care and multiple sites of care will depend on the implementation of the remaining Unique Patient Identifier components and the capability to address all of the operational requirements.

Aggregation of health information for analysis and research: The ability to support the aggregation of health information on the basis of groups of patients, regions, diseases, treatments, outcomes, etc. for research, planning and preventive

measures will depend on the implementation of the remaining Unique Patient Identifier components and the capability to address all of the operational requirements.

Support the protection of privacy, confidentiality & security
Access Security: Access Security procedures are not part of the proposal.

Content-free Identifier: Dr. Ware has revised his original position to keep the identifier content-free.

Mask/Hide/Encrypt/Protect/Disidentify: The proposal does not include encryption to protect the Identifier.

Improve health status and help reduce cost
The Unique Patient Identifier based on Bank Card Method has the potential to support the functions of a Unique Patient Identifier. However, its success depends on the implementation of the remaining Unique Patient Identifier components and the capability to address all of the operational requirements. The nation-wide implementation of a new system will require a huge investment of resource, time and effort.

VII. Strengths and Weaknesses

Strengths:

1. Meets almost all of the ASTM conceptual characteristics (of the 30 requirements, fully meets 27)

1. The Bank Card Method is a new choice and can be designed to exclude known defects or limitations.

2. It provides an opportunity to develop the required specifications and design precisely for the system to efficiently meet the industry's need.

3. It avoids crossover problems from an existing system that need to be remedied or those that cannot be corrected retrospectively.

4. The financial industry has a demonstrated success with the plastic card identification systems.

5. The experience, know-how and the capability to implement such a system is already in the private sector.

6. The necessary technology such as inexpensive card readers that respond to keystrokes or magnetic-stripe, printers etc. has already been developed.

Weaknesses:

1. Does not meet three of the five operational characteristics and does not fully address the fourth characteristic.

2. Does not meet the six identifier component requirements, including the format of the identifier (number of digits) pending development of an RFP.

3. Currently, the Bank Card Method remains only as a concept and its fruition depends upon significant planning, preparation, specification, design and development.

4. The purpose and scope of Bank Card is limited. It is used for querying balance, seeking credit approval, transmitting credit or debit transactions. All transactions are handled by the same financial institution that issued the card. While it is a good model for handling financial transactions, its potential for identifying individuals, linking and aggregating patient information from multiple provider organizations for the purpose of delivering care or research will depend on its design which is yet to be planned and developed.

5. Untested - implementing a brand new system nationwide has inherent risk for its success.

6. The required technology infrastructure and various administrative structures need to be established.

7. The method requires creation of a Central Trusted Authority, development of its organizational structure and operating procedures, definition of its authority and an implementation plan.

9. Overcoming/solving the above weaknesses will require a substantial investment of money, huge effort and a longer time frame than enhancing an existing identification system.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. The Bank Card Method is not in a ready-to-implement form. Therefore, it presents several challenges to completing the various preliminary tasks including the development of specifications, design, implementation, maintenance, etc.

2. Establishment of the Central Trusted Authority and determination of its administrative and technology infrastructure

3. The RFP process and the card industry's ability and willingness to manage the identifier for the healthcare industry

4. Cost

4. Timeliness of the solution.

IX. Solutions to the Barriers:

1) Inclusion of the missing identifier components and operational characteristics.

2) Establishment of a team of experts, recommended by Dr. Ware to develop this concept and help in:

a) the development of identifier specifications, design, etc.

b) the development and issue of the RFP recommended by Dr. Ware.

c) the establishment of a Central Trusted Authority

d) the technology infrastructure including software, hardware and communication issues

e) the implementation methodologies and policies and procedures

f) investment and implementation schedule**.**

4. Cryptography-based Patient Identifier

I. Description of the Option

Dr. Peter Szolovits from Massachusetts Institute of Technology recommends a Healthcare Identifier System based on cryptography method. It consists of the use of two keys that allow arbitrary messages to be encoded and decoded. These two keys contain mathematical functions that are inverses of each other. The patient holds a patient private-key and the provider organization holds an organizational (provider) public-key. The two keys together generate and maintain IDs that are both organization specific and unique to individual patients within that organization. The ID can be revealed to other institutions or practitioners only with the private-key of the patient.

The cryptography method supports both centralized and decentralized control. Under the decentralized system, the patient has the ultimate control over the degree to which the lifetime collection of medical information is made available to others. Every individual at birth is issued a private key and every institution receive a public key. The cryptography function computes institution specific Patient IDs using these two keys. Under the centralized system a central authority handles all private-keys via an ID Server. At the request of authorized institutions, the ID Server will generate Patient ID with the use of both the patient's private-key and the public-key. Under both centralized and decentralized systems, the use of smart card and the computer is required. A set of patient demographic identification is used to calculate the keys which are used in turn to generate Patient IDs. Based on the identification information, a digital certificate is issued to each individual which can be in the form of a smart card. The keys and IDs are hundreds (100s) of characters in length.

Due to the length and format of the ID, Dr. Peter Szolovits envisions his method to evolve over a period of time. In the initial stage, the ID will function as a component of the patient demographic information and coexist with the existing medical record number. The initial function of this digital ID will be exchanging information between organizations. It will facilitate the exchange of information without transmitting the medical record number itself, thereby protecting the identity of the individual. When the level of automation and the use of computers have become universal, the digital ID will assume the role of the primary identifier and function as the Unique Patient Identifier. To assure anonymity of care and protection of privacy, Dr. Szolovits does not recommend tracking the various points delivery of care.

Automation and use of computer technology are prerequisites for the implementation and use of the Cryptography-based Patient Identifier. It cannot be used in a manual environment. The cryptography based method is popular in the financial industry and it is used mainly to facilitate secure electronic transactions over computer networks. However, the Cryptography-based Patient Identifier is still only a concept. It needs to be developed further. Dr. Szolovits points out that the cryptography-based

public-key and private-key method is a very powerful tool, and its creative application will yield different degrees of privacy, convenience and flexibility. Therefore, the method needs to transition from the conceptual stage to specification, design, development, testing and large scale deployment in order to meet the requirements of the healthcare industry.

II. Author/Proponent and Documentation

1. The Cryptography-based Identification is already being used in the financial industry for secure electronic transactions (SET) over computer networks.

2. The method is being recommended by Dr. Peter Szolovits, Massachusetts Institute of Technology. His article published in the Journal of American Medical Informatics Association provides the outline for this method.

Compliance with ASTM Conceptual Characteristics

Dr. Szolovits points out that in the initial stage, the Cryptography based Identifier will function as a component of the medical record number to facilitate exchange of information. Until the use of computer has become universal, it will not be used as a primary patient identifier. His concept of ID Server, issuing authority, centralized and decentralized use, etc. need to be developed further to fully understand the characteristics of the Cryptography-based Patient Identifier.

a) Functional Characteristics

Accessible: Dr. Szolovits, recommends a trusted authority/institution such as a government or semi-public consortium to function as a ID Server for the issue of the Cryptography-based identifier.

Assignable: The ID will be assigned by the ID Server. Both the patient's private key and the provider organization's public key are required.

Identifiable: The trusted authority will have the necessary information to support the issue and maintenance of the Cryptography-based Patient Identifier. However, the necessary specifications, design and development are yet to be planned.

Verifiable: It should be possible for the trusted authority to verify the validity of the ID. However, no details have been included in the proposal.

Mergeable:This can be accomplished at the trusted authority level.

Splittable: This can be addressed with appropriate procedures at the trusted authority level.

b) Linkage of Lifelong Health Record

Linkable: The Cryptography-based Patient Identifier can be used to link patient records from multiple sources.

Mappable: Bidirectional linkage is possible between the Cryptography-based Patient Identifier and the existing Identifiers. The proposal expects it to be part of the patients demographic information in the initial stage.

c) Patient Confidentiality and Access Security

Content Free: The patient's private-key and an institution's public-key are based on their respective personal and demographic information.

Controllable: This method requires the trusted authority to maintain security of the private and public keys and encryption information.

Healthcare Focused: The Cryptography-based Patient Identifier proposal is healthcare focused.

Secure: This method requires the trusted authority to maintain security of the private and public keys and related information. However, the necessary policies, procedures, specifications, design and development are yet to be planned.

Disidentifiable: Encrypted identifier has the ability to hide the identity of the individual.

Public: Public disclosure of the Unique Patient Identifier without risk to privacy and confidentiality of patient information is not discussed. The private key and institution specific patient ID are not meant to be public information.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** Not based on existing Unique Patient Identifier Standards.

Deployable: The financial industry is using the cryptography method for secure electronic transactions. The Cryptography-based Patient Identifier cannot be used in a manual environment.

Usable: The identifier is in an encrypted format containing hundreds of characters. It is not suitable for manual use.

e) Design Characteristics

Unique: IDs issued are institution specific. Patients will receive different IDs from different institutions. Cryptography-based Identifiers are not unique across the nation.

Repository-based: Patients' private keys will be calculated from the patient demographic identification information. Therefore, such information can be maintained in a repository. However, its design especially relating to the issuing method (Centralized vs. Distributed) will determine its feasibility.

Atomic: The identifier itself is in the encrypted format and can be treated as a single data item.

Concise: The identifier is in the encrypted format containing hundreds of characters. Therefore, it is not concise.

Unambiguous: The identifier is in the encrypted format containing hundreds of characters. Its content will not be meaningful for manual review.

Permanent: Patients will have multiple identifiers each issued by different organizations that delivered the care. Even, within the same institution, the use of different encryption scheme will yield different identifiers.

Centrally governed: The issue and maintenance of the ID can be governed both centrally as well as in a distributed manner. They will be subject to the specification, design, development, testing and deployment that are yet to be organized.

Networked: Digital IDs, encrypted messages and transactions are currently transmitted over computer networks.

Longevity: This method can support patient identification for a foreseeable future.

Retroactive: This method can be used for retroactive assignment of identifiers.

Universal: This method can support universal use.

Incremental Implementation: Dr. Szolovits recommends an incremental implementation. In the initial stage, this ID will function as a component of the patient demographic information and coexist with the existing medical record number. The initial function of this digital ID will be exchanging information between organizations. When the level of automation and the use of computers have become universal, the digital ID will assume the role of the primary identifier and function as the Unique Patient Identifier.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: This is subject to specification, design, development, testing and deployment that are yet to be planned.

IV Compliance with Operational Characteristics

Currently operational: The Cryptography-based Patient Identifier is not currently operational.

Existing infrastructure: Does not have existing administrative or technical infrastructure.

Readiness of the required technology: The method requires the healthcare industry to increase its level of automation and use of computer in order to use the Cryptography-based Patient Identifier. According to its proponent, the initial role of this method is intended only for exchanging information between organizations.

Timeliness: The Cryptography-based Patient Identifier method is at a conceptual level and needs to be developed further. The level of automation in healthcare organizations also needs to be increased before this method can be implemented.

Adequacy of information to support identification functions: The Cryptography-based Patient Identifier is at a conceptual level. The identification data base and its contents have not yet been addressed.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
The Cryptography-based Patient Identifier is not a Unique Patient Identifier. It focuses on the use of private-key and public-key to generate an institution specific patient identifier. The keys and identifiers are of hundreds of characters in length. They are suitable for secure electronic transmission of information but, unsuitable for manual use and cumbersome for record keeping functions.

Identification Information
The Patient identification data base and its contents have not yet been addressed.

Index
The index that would link the identifier and the patient's identification information has not been addressed.

Mechanism to protect, mask or encrypt the identifier
The identifier will be in encrypted format.

Technology Infrastructure
The technology infrastructure required to support the healthcare identification functions has not been addressed.

Administrative Infrastructure
The proposal requires a trusted institution for centralized control and use of escrow

agents and trusted intermediaries for decentralized control. But it does not provide any specific solution.

VI. Compliance with Basic Functions Criteria

According to Dr. Szolovits, the main focus of this method is to make unauthorized access to large scale medical information difficult. Initially the Cryptography-based Patient Identifier will be part of the patient demographic information to facilitate secure exchange of patient care information and eventually evolve in to a patient identifier once the use of computers by healthcare has become universal. In addition, compliance with the basic functions criteria depends on the identifier's compliance with operational characteristics and the required identifier components. The cryptography method is at a preliminary stage. Currently the method does not meet all of the operational characteristics and component requirements. Therefore, its ability to perform all of the basic functions discussed below will depend upon the development of a complete proposal and inclusion of missing components and operational requirements.

Identification of individuals

Delivery of care functions: According to Dr. Szolovits, the identifier will not support these functions initially. The use of computers by healthcare organizations must become universal and their functions automated adequately.

Administrative functions: Patient identification required by practitioners, provider organizations and secondary users for administrative functions will not be supported until the use of computers by healthcare organizations becomes universal and their functions automated adequately.

Identification of information

Coordination of multi-disciplinary care processes: Multi-disciplinary functions and coordination of care processes including, ordering of procedures, medications, tests, etc., communication of results and consultations will not be supported. The use of computers by healthcare organizations must become universal and their functions automated adequately.

Organization of patient information and medical record keeping: Manual medical record keeping and automated collection, storage and retrieval of information during the course of active treatment will not be supported. The use of computers by healthcare organizations needs to become universal and their functions automated adequately.

Manual and automated linkage of lifelong health records: The focus of the cryptography method is to facilitate secure exchange of information. Therefore, it has the potential to link information and records across multiple episodes of care and multiple sites of care. However, it will depend upon the implementation of the remaining Unique Patient Identifier components and the capability to address all of the operational requirements.

Aggregation of health information for analysis and research: The aggregation of health information on the basis of groups of patients, regions, diseases, treatments, outcomes, etc. for research, planning and preventive measures will not be supported initially. The use of computers by healthcare organizations must become universal and their functions automated adequately.

Support the protection of privacy, confidentiality & security

Access Security: The Access Security and the authentication procedures needed to access the patient care information are not addressed.

Content-free Identifier: The patient's private-key and an institution's public-key are based on their respective personal and demographic information.

Mask/Hide/Encrypt/Protect/Disidentify: The identifier will be in an encrypted format.

Improve health status and help reduce cost

The method does not support several of the basic functions initially. It has the potential to facilitate secure exchange of electronic medical information and link longitudinal records. It requires the use of computers by healthcare organizations become universal and their functions automated adequately.

VII. Strengths and Weaknesses

Strengths:

1. The Cryptography-based Unique Patient Identifier meets most of ASTM criteria (of the 30 requirements, fully meets 22 and partly meets 1),.

2. It is a new choice and can be designed to exclude known defects or limitations.

3. It provides an opportunity to develop the required specifications and design a system to meet the industry's need and take advantage of current technology. .

4. It avoids crossover problems from an existing system that need to be fixed or those that cannot be fixed retrospectively.

5. The financial industry has a demonstrated success with the Cryptography Method for secure Electronic transactions.

6. The experience, know-how and the capability to develop and implement such a system is already available.

Weaknesses:

1. The Cryptography-based Patient Identifier currently does not meet four of the five operational characteristics.

2. It does not meet three of six identifier components requirements and two more are

not addressed adequately.

3. The method does not yield a Unique Patient Identifier. Patients will have multiple IDs each generated by the public key of the provider.

4. According to Dr. Szolovits, automation and application of computers by the healthcare industry must be universal for this method to become a viable patient identifier.

5 The Cryptography Method is at a conceptual level. It requires specifications, design, development, testing and deployment that are yet to be organized.

6. Untested - implementing a brand new system nationwide, that has not yet been proven has inherent risk for its success.

7. The required technology infrastructure and administrative structures need to be established.

8. The method requires creation of a Central Trusted Authority, development of its organizational structure, operating procedures, definition of its authority and an implementation plan.

9. Developing and implementing a new system without the above weaknesses will require a huge investment of resources, substantial effort and time.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. The Cryptography Method is far from being ready for implementation. Therefore, it will present several challenges to completing the various preliminary tasks including its specifications, design, development, implementation, etc.

2. The current level of automation and use of computers by healthcare organizations

3. Establishment of a Central Trusted Authority

4. Investment of significant resources

5. Timeliness.

IX. Solutions to the Barriers:

1) Inclusion of the missing identifier components and operational characteristics

2) development of identifier specifications, design, etc.

3) establishment of a Central Trusted Authority

4) development of technology infrastructure including software, hardware and communication issues

5) development of implementation methodologies and policies and procedures

6) preparation of cost-benefit analysis and an implementation schedule

7) increasing the current level of automation in healthcare organizations.

5. Unique Patient Identifier based on Personal Immutable Properties

I. Description of the Option

This method has been proposed by Drs. Paul Carpenter and Chris Chute of Mayo Clinic. It is based on an individual's immutable personal properties. Both Dr. Carpenter and Dr. Chute believe that in addition to characteristics such as uniqueness, verifiability, reliability and administrative ease, the Unique Patient Identifier (UPI) should be based on immutable personal properties rather than those which may be changed by political or personal whim (i.e. last name, town, state, country etc.). Their model consists of three universal immutable values plus a check digit. The three values are 1) a seven-digit date of birth field, 2) a six-digit place of birth code, 3) a five-digit sequence code (to identify the individual born on the same date in the same geographic area) and 4) a single-check digit. The place of birth code identifies world grid coordinates using 360 degrees for longitude and 180 degrees for latitude. Each increment of a degree represent approximately 70 square miles. Local organizations can administer the Unique Patient Identifier and forward it to an international registry such as World Health Organization.

For emergency situations a temporary UPI with the prefix "T" is recommended. This model also recommends the adoption of a base 34-character representation of the UPI for personal memory and ease of use and entry into electronic medical record of the future. Although the proposal does not address the Central Issuing Authority, it indicates the need for a central registry at an organization such as WHO to compare and link records.

Just like other proposals, the Unique Patient Identifier based on Personal Immutable Properties is also at a conceptual stage. Therefore, the method needs to progress from the conceptual stage to specification, design, development, testing and large scale deployment in order to meet the requirements of the healthcare industry.

II. Author/Proponent and Documentation

1. The Unique Patient Identifier based on Personal Immutable Properties has been proposed by Paul C. Carpenter, M.D. and Christopher Chute, M.D.

2. The method is described in their article published in JAMIA in 1994

III. Compliance with ASTM Conceptual Characteristics

a) Functional Characteristics

***Accessible*:** Local organizations can handle the issue of Unique Patient Identifier.

***Assignable*:** Requires local issuing authority to assign the Unique Patient Identifier

and forward it to an international authority such as WHO. The required specifications, design, development, testing and deployment are yet to be organized, and the establishment of a local and international authority and their functions are yet to be planned.

Identifiable: Requires the local registry organization to collect demographic data.

Verifiable: Check-digit verification is included in the proposal.

Mergeable: Requires central registry to compare information supplied by the local registry and perform the necessary linkages

Splittable: Requires central registry to compare information supplied by the local registry and take the necessary steps

b) Linkage of Lifelong Health Record

Linkable: The Personal Immutable Properties-based Unique Patient Identifier can be used to link patient records from multiple sources.

Mappable: Bidirectional linkage is possible between the Personal Immutable Properties-based Unique Patient Identifier and the existing identifiers.

c) Patient Confidentiality and Security

Content Free: The Identifier is created from personal immutable properties and therefore, is not content-free.

Controllable: The Personal Immutable Properties-based Unique Patient Identifier can be encrypted. However, encryption is not included in the proposal.

Healthcare Focused: The proposal is made for healthcare purpose.

Secure: Encryption is not addressed in the proposal. The Personal Immutable Properties-based Unique Patient Identifier can be encrypted and security can be administered by the local issuing authority.

Disidentifiable: Encryption is not included in the proposal. The Personal Immutable Properties-based Unique Patient Identifier can be encrypted in multiple ways.

Public: Public disclosure of the Unique Patient Identifier without risk to privacy and confidentiality of patient information is not discussed in the proposal. The Personal Immutable Properties-based Unique Patient Identifier contains personal information about the individual. Therefore, it is not a public information.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** Not based on industry standard.

Deployable: Does not indicate any barriers.

Usable: The model recommends the adoption of a base 34-character representation of the UPI for personal memory and ease of use and entry into electronic medical record of the future. The 19-character length and the mathematics involved will present difficulty for manual calculation and use.

e) Design Characteristics

Unique: The three immutable personal properties namely date birth, place of birth and the sequential identifier assure the uniqueness of the identifier.

Repository-based: The patient ID is made up of the patient's personal properties information. The use of other demographic identification information is not discussed in the proposal. However, there is no inherent barriers to maintaining a repository.

Atomic: This model consists of a series of three universal immutable values plus a check digit. It can be considered a single compound data element.

Concise: This model consists of a 19 character length identifier which will be difficult for manual use.

Unambiguous: The identifier uses numeric characters only and does not present ambiguity.

Permanent: The identifier is intended as a permanent identifier.

Centrally governed: The proposal recommends local organizations to issue identifiers and function as local registries and report to the central organization such as WHO.

Networked: This identifier can be operated on network.

***Longevity*:** The method is capable of functioning for a foreseeable future.

Retroactive: Unique Patient Identifiers can be assigned to existing individuals retroactively. However, the sequence code for individuals born on the same date may not be in the intended sequence while retrospectively assigning their ID.

Universal: This method can support identification of every living person for a foreseeable future.

Incremental Implementation: The proposal does not address the implementation approach. This method can be implemented incrementally.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: This is subject to specification, design, development, testing and deployment that are yet to be organized.

IV. Compliance with Operational Characteristics and Readiness

Currently operational: The Unique Patient Identifier based on Personal Immutable Properties is not currently operational.

Existing infrastructure: Administrative and technical infrastructures are not ready yet.

Readiness of the required technology: The necessary technology and check-digit methodologies are ready and available for use.

Timeliness: The proposal does not address the implementation approach. The set-up of administrative and technology infrastructures (Central Trusted Authority, software, hardware, communication network, etc.), and the development of implementation methodology, policies and procedures, etc. must be completed before the nation-wide implementation. The implementation of an entirely new system will require substantial amount of time.

Adequacy of information to support identification functions: The identification data base and its contents have not been addressed. The Unique Patient Identifier based on Personal Immutable Properties still remains only as a concept.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier

The focus of the Unique Patient Identifier based on Personal Immutable Properties is mainly on the Identifier Component. The model consists of 1) a seven-digit date of birth field, 2) a six-digit place of birth code, 3) a five-digit sequence code (to identify the individual born on the same date in the same geographic area) and 4) a single digit check-digit. For easy representation the method recommends the use of a 34 base number. The 19 character ID length and the mathematics involved will be difficult for manual calculation and use.

Identification Information

The method will require the use of a patient's identifying data elements such as name, date of birth, sex, etc. But it does not address the content or structure of the data base that will contain such data elements.

Index
The proposal indicates that both local and central registries will exist. It does not address its content or the use of an index such as a Master Patient Index.

Mechanism to protect, mask or encrypt the identifier
Does not use encryption

Technology Infrastructure
Does not have an existing technology infrastructure and is not addressed in the proposal

Administrative Infrastructure
Does not have an existing administrative infrastructure. The proposal indicates that both local and central registries will exist, but it does not include a proposal for the administrative infrastructure.

VI Compliance with Basic Functions Criteria

Compliance with the basic functions criteria depends on the identifier's compliance with operational characteristics and the identifier components requirements. The Unique Patient Identifier based on Personal Immutable Properties mainly addresses the identifier component and does not meet several of the operational characteristics. Its ability to meet the basic functions of the Unique Patient Identifier will depend on the inclusion of the remaining five components and the required operational characteristics. It will be unable to meet the basic functions discussed below without them.

Identification of individuals

Delivery of care functions: The Personal Immutable Properties based Unique Patient Identifier's capability to support the positive identification of an individual during the course of active treatment will depend on its ability to address both the implementation of the remaining identifier components and all of the operational requirements.

Administrative functions: The identifier's capability to support the identification for administrative functions required by practitioners, provider organizations, insurers, HMOs, federal health plan agencies, etc. will depend on its ability to address both the implementation of the remaining identifier components and all of the operational requirements.

Identification of information

Coordination of multi-disciplinary care processes: The identifier's capability to Support multi-disciplinary functions and coordination of care processes including, ordering of procedures, medications and tests, communication of results and consultations will depend on its ability to address both the implementation of the remaining identifier components and the operational requirements.

Organization of patient information and medical record keeping: The identifier's capability to support the manual medical record keeping and the automated collection, storage and retrieval of information will depend on its ability to address both the implementation of the remaining identifier components and the operational requirements.

Manual and automated linkage of lifelong health records: The identifier's capability to identify, organize and link information and records across multiple episodes of cares and multiple sites of care will depend on its ability to address both the implementation of the remaining identifier components and all of the operational requirements. The length of the identifier will not be conducive to manual use.

Aggregation of health information for analysis and research: The identifier's ability to support the aggregation of health information on the basis of groups of patients, regions, diseases, treatments, outcomes, etc. for research, planning and preventive measures will depend on its ability to address both the implementation of the remaining identifier components and the operational requirements.

Protection of privacy, confidentiality & security

Access Security: The Access Security and the authentication procedures needed to access the patient care information are not addressed.

Content-free Identifier: The Unique Patient Identifier based on Personal Immutable Properties is based on personal immutable properties.

Mask/Hide/Encrypt/Protect/Disidentify: Does not include encryption protection

Improve health status and help reduce cost

The method has the potential to support the functions of a Unique Patient Identifier. However, it will depend upon the implementation of the remaining Unique Patient Identifier components and the capability to address all of the operational requirements. The establishment of both the administrative and technology infrastructures, the design and development of computer software, hardware and communication networks, and the implementation of security measures, etc. will require substantial investment of resource, time and effort.

VII. Strengths and Weaknesses

Strengths:

1. The Unique Patient Identifier based on Personal Immutable Characteristics meets most of the conceptual characteristics of ASTM (of the 30 requirements, fully meets 23 and partly meets 1).

2. It is a new choice that provides a new start and can be designed to exclude known defects or limitations.

3. It provides an opportunity to design, develop and implement a system to accurately meet the healthcare industry's need.

4. It avoids crossover problems from an existing system that need to be fixed or those that cannot be fixed retrospectively.

Weaknesses:

1. The Unique Patient Identifier based on Personal Immutable Characteristics in its current form does not meet three of the five operational characteristics and the fourth is not fully addressed.

2. It does not meet four of the six identifier components requirements and a fifth is not addressed adequately.

3. It remains only as a concept and its fruition will depend on significant planning, preparation, specification development, design, testing and implementation.

4. Untested - implementing a brand new system nationwide that has not been proven has inherent risk for its success.

5. The required technology infrastructure and administrative structures need to be established.

6. The method also will require the development of an implementation plan, creation of the necessary operating procedures, the definition of power and organizational structure of the Local/Central Trusted Authority, and the role of the World Health Organization (WHO), if any.

7. The Unique Patient Identifier based on Personal Immutable Characteristics is not content-free. It contains the patient's date of birth and place of birth.

8. Development and implementation of this new method, after overcoming the above weakness require a huge investment of financial resources, substantial effort and time.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. The Unique Patient Identifier based on Personal Immutable Characteristics option is not ready for implementation. Therefore, it will present several challenges to completing the various preliminary tasks including the nation-wide system design, development and implementation.

2. Establishment of a Central Trusted Authority

3. Cost

4. Timeliness

IX. Solutions to the Barriers:

1. Inclusion of the missing identifier components and operational characteristics

2. Development of identifier specifications, design, etc.

3. Establishment of a Central Trusted Authority and the role of the WHO

4. Development of technology infrastructure including software, hardware and communication issues

5. Development of implementation methodologies, policies and procedures

6. Analysis of cost effectiveness and implementation schedule**.**

6. Unique Patient Identifier based on Biometrics

I. Description of the Option

Biometric identification consists of patients' personal physical characteristics such as finger print, retina scan, iris scan, voice and DNA analysis. Some of the concerns relating to this option are organ transplant, amputation and diseases affecting organs (such as retinopathy). Biometric identification has been used by government agencies such as law enforcement and immigration. The photo included in an individual's driver's licence or employee ID, thumb print in legal documents, etc. are examples of Biometric Identification. Video-graphed, photographed or scanned image will be used for identification. It can be stored in digitized format in computers and ID Cards. Both for the issue and verification, the individual must be present. The process requires special purpose equipment such as scanner, video camera, computer and card readers with the necessary matching algorithms.

II. Author/Proponent and Documentation

1. Biometric Identification has been in use for a long period of time in various fields such as law enforcement, department of transportation, etc.

III. Compliance with ASTM Conceptual Characteristics

a) Functional Characteristics

***Accessible*:** For accessibility, this method requires the establishment of a local issuing mechanism for the identifier and a central administration to handle its nationwide scope.

***Assignable*:** In addition to the establishment of a local issuing mechanism and a central administration, the physical presence and cooperation of patients, the necessary tools and equipment such as scanner, video, etc. must all be present and functional.

Identifiable: The physical characteristics used in the Unique Patient Identifier based on Biometrics can be matched with the physical characteristics of the individual it identifies. However, additional information such as name, date of birth, etc. must also used in the identification data base.

Verifiable: Verification of the identifier will depend on the computer algorithm and equipment used

Mergeable: Duplicate IDs can be merged via cross-referencing

Splittable: Same ID issued to more than one individual can be handled by issuing

new IDs to both or one of the individual.

b) Linkage of Lifelong Health Record

Linkable: The Unique Patient Identifier based on Biometrics can be used to link patient records from multiple sources.

Mappable: Bidirectional linkage is possible between the Unique Patient Identifier based on Biometrics and the existing Identifiers.

c) Patient Confidentiality and Security

Content Free: Biometric Identifier is based on the personal information of the individual.

Controllable: It is possible to encrypt the Unique Patient Identifier based on Biometrics. However, this capability is subject to the appropriate specifications, design and development that are yet to be organized.

Healthcare Focused: Biometric Identifiers are used in other industries too.

Secure: It is possible to use encryption and the local issuing entity or a central administration can handle the security of the encryption scheme.

Disidentifiable: It is possible to encrypt the Unique Patient Identifier based on Biometrics.

Public: Biometric Identifier consists of personal information, therefore, not meant to be public.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** There is no national standard for the issue, maintenance and use of Biometric Identifiers.

Deployable: The necessary technology and processes to issue, maintain and use the Biometric Identifiers are available but, considered expensive, time consuming and cumbersome.

Usable: Other than an individual's photograph, the Biometric Identifier is not conducive to manual processing.

e) Design Characteristics

The creation, maintenance and use of Biometric Identifiers such as photo, thumb print, DNA analysis, retina scan, etc. will require special equipment, processes and procedures. They will be required both at the issuing and the verification points. In addition, adequate communication and computer capabilities will be required by all

users of the ID. Therefore, a Central Trusted Authority to oversee the operation with the necessary administrative and technology infrastructure is necessary.

Unique: The information contained in the Identifiers is unique.

Repository-based: Biometric Identification is usually supplemented by other demographic information such as name, address, etc. It can be based on a repository of identification information.

Atomic: The Unique Patient Identifier based on Biometrics can be considered as a single data item.

Concise: Biometric Identifiers are usually not concise. Digitized images will require large amount of storage.

Unambiguous: Other than an individual's photograph, the Biometric Identifier is not conducive to manual processing or recognition.

Permanent: The Unique Patient Identifier based on Biometrics is intended to be permanent. However, amputation, organ transplantation, etc. can directly affect the Biometric Identifier (i.e. Thumb Print, Retina Scan, DNA Analysis).

Centrally governed: The Unique Patient Identifier based on Biometrics requires both local issuing mechanism and a central administration.

Networked: The Biometric Identification System can be supported by computer networks.

Longevity**:** Biometric Identifiers do not use numbering system and can be used for a foreseeable future.

Retroactive: The Unique Patient Identifier based on Biometrics can be assigned retroactively to all existing individuals.

Universal: The Unique Patient Identifier based on Biometrics can be assigned to all living individuals for a foreseeable future.

Incremental Implementation: The Unique Patient Identifier based on Biometrics can be implemented incrementally.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: Biometric Identification is generally considered expensive and cumbersome to use.

IV. Compliance with Operational Characteristics and

Readiness

Currently operational: The Unique Patient Identifier based on Biometrics is not currently operational.

Existing infrastructure: Does not have existing administrative and technical infrastructures.

Readiness of the required technology: The necessary scanning and video technology, voice and DNA analysis technology are available.

Timeliness: Biometric Identification is generally considered cumbersome and time consuming to issue, maintain and use. It will require longer time period to implement than other options.

Adequacy of information to support identification functions: The identification data base and its contents have not yet been addressed.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
There are several options available for a biometric identification such as finger print, retina scan, iris scan, voice, DNA analysis, etc. Scanned or video graphed images serve as the identifier. The actual choice or choices from these various methods for use in healthcare have not been made.

Identification Information
Biometric identifier will require identifying data elements such as name, data of birth, etc., to support healthcare functions. But a proposal addressing these identification information is non-existent.

Index
An index that links the identifier and the identification information would be necessary. But a proposal addressing such an index is not in existence.

Mechanism to protect, mask or encrypt the identifier
Encryption is not being proposed for this option.

Technology Infrastructure
Does not have the required technology infrastructure in place to support healthcare functions, nor does a proposal for its creation exist.

Administrative Infrastructure
Does not have the required administrative infrastructure in place to support healthcare functions, nor does a proposal for its creation exist.

VI. Compliance with Basic Functions Criteria

Biometrics identifiers are currently used for applications that require positive identification of individuals. They are quite suitable for low volume activities such as personal identification verification. But their use in high volume transactions processing such as record keeping, information management, report generation, manual and or electronic exchange of information, coordination of multi-disciplinary team work and sensitive and timely healthcare delivery functions have not been tried. The Unique Patient Identifier based on Biometrics does not meet several of the operational characteristics and the identifier components requirements. Its ability will depend on the development of a complete proposal and inclusion of missing components and operational requirements. It will be unable to meet the basic functions discussed below without them.

Identification of individuals

Delivery of care functions: The ability to support the manual and automated identification of an individual during the delivery of care processes will depend on the format and content of the identifier, its ease of use, the turn around time, implementation of the remaining identifier components and the ability to meet all of the operational requirements.

Administrative functions: The ability to support the identification required by practitioners, provider organizations and secondary users for administrative functions will depend on the format and content of the identifier, its ease of use, the turn around time, implementation of the remaining identifier components and the ability to meet all of the operational requirements.

Identification of Information

Coordination of multi-disciplinary care processes: Multi-disciplinary functions and coordination of care processes including, ordering of procedures, medications, tests, etc., communication of results and consultations will depend on the format and content of the identifier, its ease of use, the turn around time, implementation of the remaining identifier components and the ability to meet all of the operational requirements.

Organization of patient information and medical record keeping: Manual medical record keeping and automated collection, storage and retrieval of information during the course of active treatment will depend on the format and content of the identifier, its ease of use, the turn around time, implementation of the remaining identifier components and the ability to meet all of the operational requirements.

Manual and automated linkage of lifelong health records: This ability will depend on the format and content of the identifier, its ease of use, the turn around time, implementation of the remaining identifier components and the ability to meet all of the operational requirements.

Aggregation of health information for analysis and research: The aggregation of health information on the basis of groups of patients, regions, diseases, treatments, outcomes, etc. for research, planning and preventive measures will depend on the format and content of the identifier, its ease of use, the turn around time, implementation of the remaining identifier components and the ability to meet all of the operational requirements.

Support the protection of privacy, confidentiality & security

Access Security: The Access Security and the authentication procedures needed to access the patient care information are not addressed.

Content-free Identifier: The identifier contains the patient's physical identification characteristics.

Mask/Hide/Encrypt/Protect/Disidentify: Encryption is not addressed.

Improve health status and help reduce cost

The method appears to lack the ability to support several basic functions. It is missing several operational characteristics and identifier components. The inclusion of missing characteristics, establishment of both the administrative and technology infrastructures, design and development of computer software, hardware, and communication networks, and implementation of security measures, etc. will require substantial investment of resources, time and effort.

VII. Strengths and Weaknesses

Strengths:

1. The Unique Patient Identifier based on Biometrics meets most of the ASTM conceptual characteristics (of the 30 requirements, fully meets 20 and partially meets 3).

2. It has the potential to provide positive identification of the patient.

3. It avoids crossover problems from an existing system that need to be remedied or those that cannot be corrected retrospectively

Weaknesses:

1. The Unique Patient Identifier based on Biometrics in its current form does not meet three of the five operational characteristics and the fourth one is not fully addressed.

2. It does not meet four of the six identifier components requirements and the remaining two are not addressed adequately.

3. Verification of the identifier requires special equipment, computer software, and expertise (DNA analysis, Finger Print, Retina Scan, etc.).

4. Verification process for the identifier requires longer period of time (DNA analysis, Finger Print, Retina Scan, etc.) and can affect the timely delivery of care.

5. Biometric Identification is generally considered cumbersome and time consuming to issue, maintain and use. It requires longer time period to implement than other options.

6. Since the Biometric Identifier contains an individual's personal characteristics and information, the risk of violation of privacy and confidentiality is greater than that of other options.

7. While Biometric Identifiers have proven to be a good option for Law Enforcement and Immigration and Naturalization departments, its potential for identifying individuals, linking and aggregating patient information from multiple provider organizations for the purpose of delivering care or research will depend upon its design which is yet to be planned and developed.

8. Untested - implementing a brand new system nationwide that has not been proven in healthcare industry has inherent risk for its success.

9. The required technology infrastructure and administrative structures need to be established.

10. The method requires creation of a Central Trusted Authority, development of its organizational structure and operating procedures, definition of its authority and an implementation plan.

11. Overcoming/solving the above weaknesses will require a substantial investment of money, huge effort and a longer time frame.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. Inclusion of the missing identifier components and operational characteristics

2. Biometric Identifiers contain personal characteristic information. It poses threat to the violation of an individual's privacy.

3. Unique Patient Identifier based on Biometrics is not ready for implementation. It will present several challenges to completing the various preliminary tasks including the nation-wide system design, development and implementation.

4. Establishment of the Central Trusted Authority and determining the required administrative and technology infrastructure

5. Cost

6. Timeliness.

IX. Solutions to the Barriers:

1. Selection of a choice from among the different biometric identification methods

2. Development of identifier specifications, design, etc.

3. Establishment of a Central Trusted Authority

4. Development of technology infrastructure including software, hardware and communication issues

5. Development of implementation methodologies, policies and procedures

6. Preparation of a cost-benefit analysis and an implementation plan.

7. Lifetime Human Service & Treatment Record (LHSTR) Number based on Birth Certificate

I. Description of the Identifier

Edward F. Hernandez, Bureau of Records and Statistics, San Francisco Department of Public Health recommends a Lifetime Human Service & Treatment Record Number which will serve as a Unique Patient Identifier. Birth Certificates are personally specific and uniquely enumerated. The national civil registration consists of three components. They are:

1) registration in birthing hospitals (Birth Certificate)

2) "Official Report of Birth" in the case of an US citizen giving birth or fathering or adopting a child outside the territorial boundaries of US

3) alien registration document or "green card" and other forms of the U.S. Visa issued by the Department of State.

Of these three disparate components, the Birth Certificate is the largest and the other two serve as its surrogate. Although each one of them uses different enumeration method, all of their documents exist in both paper and electronic formats. Mr. Hernandez' proposal consists of linking these documents to a randomly assigned 16-digit number. A *personal identification number* or "PIN" chosen by individuals or their designee would also be included. A 16-digit ID number can support 10^{15} (ten quadrillion) individual numbers and a 16-position alphanumeric ID can support 16^{16} individual unique Identifiers. The above three components that provide factual basis for the establishment of a LHSTR are divided into three breeder (document) types. The method also includes a six-digit check-digit verification and a public-key/private-key based encryption on an as needed basis.

The LHSTR file structure includes a three tier approach. A set of seven core data elements forms the first order of document. It consists of:

1. sixteen (16) position randomly assigned permanent identifier (LHSTR Number)

2. the full name of the individual as stated in the document

3. date of birth as stated in the document

4. place of birth as stated in the document

5. mother's name as stated in the document

6. enumerator on the document

7. type of the document.

The second order documents includes a longitudinal component supplementing the basic record to corroborate over time to protect against error or fraud of the association between the individual and the record. They include U.S. passport, social security record, a state driver license, military ID, etc. The third order of documents consists of medical or social service record. The purpose is to facilitate event-by-event tracking of all health and human services provided to an individual on an explicit and consensual basis. The content includes type of service, provider ID and date and time of service. The event-by-event data can be captured through a point-of-sale (POS) terminal with the recipient using a card and PIN or manual entry in the POS terminal. The third order of documents may also include those documents that were created on the basis of the second order of documents such as a membership card, ATM Card, library card, etc. In the case of an emergency, if identifiers are not available, a temporary record must be created and resolved later after the identity is established. Mr. Hernandez is currently working on improving this model further. He recommends the creation of a national level organization to oversee the LHSTR operation . He suggests that the current Association of Vital Records and Health Statistics that exists in the 50 states can be organized into a United States Vital Health Records Trust to function as a Central Trusted Authority. He also recommends the United States Postal Service, SSA, Local Public Health Authorities, etc. as other possible options.

II. Author/Proponent and Documentation

1. Edward F. Hernandez, Director Bureau of Records and Statistics, San Francisco Department of Public Health UHID is the proponent of this method.

2. Mr. Hernandez has provided a document that outlines his method in detail.

III. Compliance with ASTM Conceptual Characteristics

a) Functional Characteristics

***Accessible*:** The LHSTR Number requires a Central Trusted Authority for its issue and maintenance.

***Assignable*:** The LHSTR Number proposal includes a Central Trusted Authority for its assignment. However, the necessary policies and procedures for its access and assignment, the required specifications, design, development and testing for its implementation, the establishment of a local and international authority and the definition of their functions and responsibilities are yet to be planned.

Identifiable: LHSTR Number will be supported by three levels of patient identification data including tracking of event-by-event healthcare service rendered along with provider information.

Verifiable: The proposal includes a six (6) digit check-digit verification process.

Mergeable: Duplicate LHSTR Numbers can be merged at the Central Trusted Authority level with appropriate policies and procedures via cross-referencing.

Splittable: Same ID issued to more than one individual can be handled by issuing new IDs to both or one of the individual.

b) Linkage of Lifelong Health Record

Linkable: The LHSTR Number can be used to link patient records from multiple sources.

Mappable: Bidirectional linkage is possible between the LHSTR Number and the existing Identifiers.

c) Patient Confidentiality and Access Security

Content Free: The LHSTR Number is free of information about the individual.

Controllable: The public-key/private-key information and encryption scheme can be controlled at the Central Trusted Authority level.

Healthcare Focused: The LHSTR Number is solely for the purpose of healthcare.

Secure: The public-key/private-key information and encryption scheme can be controlled at the Central Trusted Authority level.

Disidentifiable: The initial LHSTR Number draft proposal uses encryption based on public-key/private-key.

Public: The LHSTR Number is content-free. The public disclosure of the Unique Patient Identifier without risk to privacy and confidentiality of patient information is not discussed in the proposal. However, patient identifiers are not public information.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** The Identifier is not based on existing standards.

Deployable: The LHSTR Number is capable of implementation in a variety of technologies such as scanners, bar code readers, etc.

Usable: The LHSTR Number is capable of implementation in a variety of technologies such as scanners, bar code readers, etc. The 22 digit identifier will be difficult for manual use.

e. Design Characteristics

Unique: The LHSTR Number is intended to be a unique number nationally.

Repository-based: LHSTR Number is repository-based. It is supported by three levels of patient identification data including the tracking of event-by-event healthcare service rendered along with provider information.

Atomic: The LHSTR Number can function as a single data element.

Concise: The 22 digit length is not concise for manual use and memory.

Unambiguous: The LHSTR Number proposal provides a choice of numeric and alphanumeric characters. Zeros and ones could present some ambiguity with alphabets "o" and "l".

Permanent: The LHSTR Number is intended as a permanent identifier. It can support 16^{16} unique numbers.

Centrally governed: The LHSTR Number approach requires a Central Trusted Authority and its proponent, Mr. Hernandez recommends the creation of an organization called United States Vital Health Records Trust.

Networked: The LHSTR Number can be operated on a computer network.

Longevity**:** Can support patient identification for a foreseeable future. The sixteen digit numbering system can support 16^{16} unique IDs.

Retroactive: Has the capacity for retroactive assignment of the LHSTR Number to each person in the United States.

Universal: Can support identification of all living individuals for a foreseeable future.

Incremental Implementation: The LHSTR Number can be implemented on an incremental basis. With the development and use of appropriate procedures both the LHSTR Number and existing patient identifiers can co-exist during the time of transition with the establishment of necessary bidirectional mapping.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: The LHSTR Number has the potential to support the identifier functions and enhance the health status of the nation through efficient record keeping and management, sharing of information, reduced cost of integration and optimum use of technology. The establishment of both the administrative and technology infrastructures, the creation of the Trusted Authority, the design and development of computer software and hardware, and the design and development of communication

networks and security measures will require substantial expenditure.

IV. Compliance with Operational Characteristics and Readiness

Currently operational: The LHSTR Number is not currently operational.

Existing infrastructure: Does not have existing administrative and technical infrastructures.

Readiness of the required technology: The necessary technology and methodologies are ready and available for use.

Timeliness: The LHSTR proposal consists of randomly assigning a 16 digit identifier to each of the three existing civil breeder records without the need for the participation of individuals. The individuals will pick a personal identification number (PIN) similar to the PIN used with ATM Bank Cards to guard against unauthorized use. However, the implementation of an entirely new system including the creation of administrative and technology infrastructures (Central Trusted Authority, software, hardware, communication network, etc.) and development of policies and operating procedures requires substantial amount of time and resource.

Adequacy of identification information to support identification functions: The LHSTR Number proposal includes a three tier identification information that includes 1) identification information about an individual that does not change, (DOB, Mothers Name, etc.) 2) those that are acquired longitudinally (e.g.. SSN, Drivers License Number, etc.) and 3) medical service data (provider ID, type of service, date of service, etc.).

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
The LHSTR proposal includes a 16 digit randomly assigned identifier, a 6 digit check-digit and a six digit optional encryption scheme.

Identification Information
LHSTR Number proposal includes a three tier identification information that includes 1) permanent identification information that do not change, 2) those that are acquired over one's life time and 3) medical service data (provider ID, date of service, etc.).

Index
The LHSTR serves as the index.

Mechanism to protect, mask or encrypt the identifier

A public-key/private-key based encryption is included in the proposal with the option to choose a different method if needed.

Technology Infrastructure
The technology infrastructure such as software, communication network, hardware, etc has not been addressed.

Administrative Infrastructure
Mr. Hernandez recommends that the current Association of Vital Records and Health Statistics that exists in the 50 states can be organized into a United States Vital Health Records Trust to function as a Central Trusted Authority. He also lists the USPS, SSA, local public health authorities, etc. as possible options.

VI. Compliance with Basic Functions Criteria

Compliance with the basic functions criteria depends upon the identifier's compliance with operational characteristics and the identifier components requirements. The LHSTR Number proposal complies with 2 of the 5 operational characteristics more than 4 of the 6 identifier component requirements. The proposal must comply with all of the components and operational characteristics to fulfill the basic functions discussed below. LHSTR 29/22 character length is unsuitable for manual use. Therefore, at best it can only partially meet the Unique Patient Identifier's basic functions.

Identification of individuals

Delivery of care functions: The LHSTR Number has the potential to support the positive identification of an individual required during the course of active treatment subject to the successful implementation of remaining components and operational requirements. However, the length of the identifier will be difficult for patients to remember and users to process manually.

Administrative functions: The LHSTR Number has the potential to support the identification for administrative functions required by practitioners, provider organizations, insurers, HMOs, federal health plan agencies, etc. subject to the successful implementation of remaining components and operational requirements. However, the length of the identifier will not be conducive to manual use by patients, providers, payers, etc.

Identification of information

Coordination of multi-disciplinary care processes: The LHSTR Number has the potential to support multi-disciplinary functions and coordination of care processes including, ordering of procedures, medications and tests, communication of results and consultations subject to the successful implementation of remaining components and operational requirements. However, the length of the identifier will present difficulty in manual use, such as verbal communication, telephone enquiry and

personal interactions.

Organization of patient information and medical record keeping: The LHSTR Number has the potential to support automated collection, storage and retrieval of information subject to the successful implementation of remaining components and operational requirements. However, the length of the identifier will not be conducive to manual use. Currently, most of the provider organizations are required to maintain manual medical records in addition to electronic information.

Manual and automated linkage of lifelong health records: The LHSTR Number has the ability to identify, organize and link information and records across multiple episodes of cares and multiple sites of care subject to the successful implementation of remaining components and operational requirements.

Aggregation of health information for analysis and research: The LHSTR Number has the ability to support the aggregation of health information on the basis of groups of patients, regions, diseases, treatments, outcomes, etc. for research, planning and preventive measures subject to the successful implementation of remaining components and operational requirements.

Support the protection of privacy, confidentiality & security

Access Security: The Access Security and the authentication procedures needed to access the patient care information are not addressed.

Content-free Identifier: The LHSTR Number is a content-free identifier.

Mask/Hide/Encrypt/Protect/Disidentify: The LHSTR Number proposal includes encryption to protect the Identifier. This capability subject to the successful implementation of remaining components and operational requirements.

Improve health status and help reduce cost

The LHSTR Number has the potential to support the functions of a Unique Patient Identifier. It is contingent upon the establishment of both the administrative and technology infrastructures, the creation of the Trusted Authority, the design and development of computer software, hardware and communication networks and the implementation of security measures which will require substantial investment of resource, time and effort.

VII. Strengths and Weaknesses

Strengths:

1. The LHSTR Number meets most of the ASTM conceptual characteristics effectively (of the 30 requirements, fully meets 24 and partly meets 2). .

2. It meets three of the five operational characteristics.

3. It meets four of the six identifier components' requirements. It also meets the fifth one partially.

4. It meets both the basic functions criteria and the privacy, confidentiality and security criteria effectively.

5. Avoids crossover problems from an existing system that need to be corrected or those that cannot be corrected retrospectively.

6. The three (3) components of the civil registration namely, birthing hospital registries, the official report of birth and the alien registration documents together have the maximum potential to enumerate all individuals living in the nation for the issue of the 16 digit LHSTR Number.

7. The three (3) level data segments that support the LHSTR Number can provide both a reliable identification with a high degree of accuracy and the necessary information about a patient's previous episodes of care and medical records relating to them.

8. This is the only option that provides patient participation with PIN security.

9. Provides an opportunity to design an identification system that can take advantage of emerging technologies and available resources

10. Offers capacity to handle the nation's population for a foreseeable future.

Weaknesses:

1. LHSTR Number is at a conceptual level.

2. Untested - implementing a brand new system nationwide has inherent risk for its success.

3. Lack of existing infrastructure - technology and administrative infrastructures need to be established afresh.

4. Lack of existing plan and procedures - LHSTR Number requires the development of an implementation plan for the establishment of necessary infrastructure including the establishment of a trusted authority, definition of its power, organizational structure, operating procedures, etc.

5. Significant cost - planning, design, development and implementation of the LHSTR Number will require a substantial investment of resources, a huge effort and a longer time frame.

VIII. Potential Barriers & Challenges to Overcoming the

Barriers

1. Establishment of a Central Trusted Authority

2. Substantial investment

3. Timeliness.

IX. Solutions to the Barriers:

1. The LHSTR Number is at a conceptual stage. It will present several challenges to completing the various preliminary tasks including the nation-wide system design, development and implementation.

2. Development of identifier specifications, design, etc.

3. Establishment of a Central Trusted Authority

4. Development of the necessary technology infrastructure including software, hardware and communication protocols

5. Development of implementation methodologies, policies and procedures.

6. Analysis of the cost-effectiveness and feasibility of timely implementation.

8. Existing Medical Record Number (MRN) based identification

I. Description of the Option

The current method of identifying a patient and patient information by the majority of organizations is based on the use of Medical Record Numbers. Each provider organization maintains a Master Patient Index (MPI) and the Medical Record Number is issued and maintained through this index. The MPI usually contains the patient's demographic information such as name, date of birth, address, mother's maiden name, SSN, etc. The Medical Record Number is used to identify an individual and his or her medical record/information. It is designed to be unique only within the same organization. The numbering system including the content and format of the medical record number is usually specific to the individual organization. Patients and providers will be required to use the respective Medical Record Number when dealing with different provider organizations. Recently, Hospital Information Systems vendors introduced the Enterprise-wide Master Patient Index which facilitates the mapping of a patient's Medical Record Number from one institution to another within the same enterprise. Since the Medical Record Numbers is unique only within the same organization, it does not adequately support access among multiple organizations or across the national healthcare system.

In order to facilitate queries and communication among these provider specific MPIs, software based solutions are being planned. Patient Identification Service by CORBAMed and HL7 MPI Mediation by HL7 are two initiatives that are currently underway. They are discussed in this report as alternatives to Unique Patient Identifiers. However, representatives involved in them indicate that in addition to the local identifier, a Unique Patient Identifier and a Central Trusted Authority are desirable to achieve their objectives fully.

II. Author/Proponent and Documentation

1. Medical Record Number, also known as Unit Number and Patient Number is the current method of patient identification being used for purposes including delivery of care, record keeping and communication.

2. Healthcare Organizations have the necessary policies and procedures in place for the use and management of Medical Record Numbers.

III. Compliance with ASTM Conceptual Characteristics

a) Functional Characteristics

***Accessible*:** Identifiers are issued and maintained by the provider organization itself.

***Assignable*:** Identifiers can be assigned by the provider organization itself.

Identifiable: The MPI maintained by provider organizations contain the necessary identification information.

Verifiable: Organizations with computerized issue of Medical Record Numbers have the check-digit verification capability.

Mergeable: Duplicate Medical Record Numbers are one of the problems facing the current institutional MPIs. Prevention of the issue of multiple Medical Record Numbers has been a challenge and the merger of the respective records a persistent problem in healthcare organizations. Merger is accomplished through cross-referencing.

Splittable: Instances of the same Medical Record Number assigned to multiple individuals are fewer in relation to duplicate issues. However, the ability to split the same medical record number assigned to multiple individuals faces the same problems as merging duplicate numbers and records. New numbers are issued to one or all individuals that have the same number.

b) Linkage of Lifelong Health Record

Linkable: Medical records within the same organization are linked together under the same Medical Record Number. However, the institution specific Medical Record Number does not provide adequate support to track or link medical records from multiple organizations or facilitate the electronic exchange of patient information.

Mappable: Does not apply; MRN is not a new identifier proposal.

c) Patient Confidentiality and Security

Content Free: Organization based MRNs are usually content free.

Controllable: Does not use encryption or decryption scheme to hide the identity of the individual

Healthcare Focused: MRN is healthcare focused.

Secure: Does not use encryption nor requires a trusted authority to enforce a secure identifier

Disidentifiable: Does not use encryption or decryption scheme to hide the identity of the individual

Public: MRN is not intended to be public information and will require access security protection.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** Not based on standards. Medical Record Numbers have been in use for a long period of time. Many policies and procedures have been developed and implemented based on them.

Deployable: MRN is compatible with technologies such as bar code readers, scanners, etc.

Usable: There is no inherent barriers to the usability of the MRN by both manual and automated means..

e) Design Characteristics

Unique: Intended to be unique only within the same organization. Patients will have multiple Medical Record Numbers each issued by different organization providing care.

Repository-based: The Master Patient Index used in hospitals and provider organizations serve as the repository.

Atomic: The organization based MRN is atomic.

Concise: The organization based MRN is concise.

Unambiguous: Existing organization based MRN consists of numeric digits. Zeros and ones may present some ambiguity with letters "o" and "l" respectively.

Permanent: Patients will have multiple identifiers each issued by different organizations that delivered care. Within the same institution the identifier will be unique.

Centrally governed: The issue and maintenance of MRN s are managed by the provider organization itself.

Networked: MRNs are used within the same organization. There are no barriers to implementing it over a network.

***Longevity*:** The scope of the MRN is limited to the same organization.

Retroactive: Does not apply. MRN is currently in use and not a new identifier proposal.

Universal: The scope of the organization-based MRN is not universal. It is intended only for patients visiting the organization.

Incremental Implementation: MRNs are already in use.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: This option leaves the existing method of identification in tact. Therefore, it will not require any new expenditure for implementation. On the other hand, it will preserve the status quo and not effect any change in the cost or the health status of the nation.

IV. Compliance with Unique Patient Identifier's Operational Characteristics

Currently operational: MRN is not currently operational as a Unique Patient Identifier.

Existing infrastructure: Does not have national level administrative or technical infrastructures. MRN is administered by respective provider organizations and it is unique only within the same organization.

Readiness of the required technology: The software initiative to facilitate query and communication among MPIs is the planning stage.

Timeliness: The effort to convert MRNs to be unique nationally or establish linkage or communication among independent institutional MPIs requires extensive planning, effort and enormous amount of time.

Adequacy of information to support identification functions: The organization-specific MPI does not contain information regarding records residing in other provider organizations.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
MRN is organization-specific. It is not a Unique Patient Identifier. It is unique only within the organization that issued it.

Identification Information
The patient's demographic information collected and maintained by provider organizations are accessible for use only within the same organization.

Index
The Master Patient Index currently used by provider organizations are specific to respective organizations. They are not mappable to the same individual's MRN in another organization.

Mechanism to protect, mask or encrypt the identifier
Encryption is not part of the current Medical Record Number.

Technology Infrastructure
The scope of the technology infrastructure is limited to operation within the same provider organization.

Administrative Infrastructure
The scope of the administrative infrastructure is limited to operation within the same provider organization.

VI. Compliance with Basic Functions Criteria

Access to geographically-distributed information requires the patient identifier to expand beyond an institutional level. The existing institution-based MRNs are adequate to manage the patient identification only within that institution. A robust identification method that can identify individuals uniquely across the nation and facilitate the linkage of their lifelong health record is the main objective of the Unique Patient Identifier. The institution-based MRN is not a Unique Patient Identifier. It does not comply with the Unique Patient Identifier's operational characteristics and component requirements. In the absence of these critical elements, the MRN lacks the ability to fulfill the basic functions discussed below.

Identification of individuals

Delivery of care functions: MRN is not a Unique Patient Identifier that can support identification across multiple organizations. The positive identification of an individual during delivery of care is possible only within the organization that issued the identifier.

Administrative functions: The identification for administrative functions required by practitioners, provider organizations, insurers, HMOs, federal health plan agencies, etc. is possible only within the organization that issued the identifier.

Identification of information

Coordination of multi-disciplinary care processes: The support for multi-disciplinary functions and coordination of care processes including ordering of procedures, medications and tests and communication of results is possible only within the organization that issued the identifier.

Organization of patient information and medical record keeping: The support for manual medical record keeping and automated collection, storage and retrieval of information during the course of delivery of care is possible only within the organization that issued the identifier.

Manual and automated linkage of lifelong health records: The MRN lacks the ability to identify, organize and link information and records across multiple episodes and sites of care.

Aggregation of health information for analysis and research: The Medical Record Number lacks the ability to support the aggregation of health information across multiple episodes from multiple providers for research, planning and preventive measures.

Protection of privacy, confidentiality & security

Access Security: Access Security procedures are applicable only within organization that issued the identifier.

Content-free Identifier: The Medical Record Number is content-free.

Mask/Hide/Encrypt/Protect/Disidentify: Does not use encryption.

Improve health status and help reduce cost

The Medical Record Number will retain status quo and not yield a Unique Patient Identifier solution to access across multiple providers, the creation of longitudinal record, etc.

VII. Strengths and Weaknesses

Strengths:

1. Already operational

2. Eliminates the effort, time and investment that will be required for developing and implementing a new identifier

Weaknesses:

1. The existing Medical Record Number is not a Unique Patient Identifier.

2. Meets only 14 of the 30 ASTM conceptual requirements fully

3. Does not meet four of the five operational characteristics and none of the Unique Patient Identifier components' requirements

4. Does not fulfill the basic functions of a Unique Patient Identifier adequately

5. The existing medical record numbers are not able to support exchange of information across institutional boundaries. Although, use of an enterprise-wide MPI offers some help within an enterprise, the need for communication beyond an enterprise in turn led the industry in search for a Unique Patient Identifier.

6. Sophisticated computer tools and software have to be developed and implemented to address the exchange of information from multiple institutions with multiple identifiers for the same patient. This task has been an unfulfilled challenge for the industry.

7. Does not support tracking of a patient's other sites of care or record locations.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. Successful development of software applications to provide exchange of patient care information based on multiple Medical Record Number among multiple provider organizations nation-wide

2. Ability to track patients' other sites of care and record locations

3. Timely development of software applications to facilitate communication among MPIs

4. User acceptance.

IX. Solutions to the Barriers:

Existing Medical Record Numbers are institution-specific and do not support identification across institutional boundaries. Therefore, successful development of software applications and communication technologies to track the various sites of care and to provide exchange of patient care information based on multiple Medical Record Numbers among multiple provider organizations nation-wide can facilitate the continued use of Medical Record Numbers.

9. Identification based on Medical Record Number and Provider Prefix

I. Description of the Option

Peter Weagaman from Medical Record Institute (MRI) proposes that a patient identifier must first and foremost identify the patient record and the focus be directed away from patient identification to identification of the patient information. In order to achieve a unique patient database identification, the Medical Record Institute proposes the use of existing provider institution generated medical record number with a provider number prefix. The solution requires consensus on a practitioner identification system but eliminates the cost of creating, implementing and maintaining a nationwide (patient) numbering system. The unique provider ID would identify the location of the patient database and the medical record number would identify the patient's record within that database. The proposal also includes designation by the patient of a practitioner of choice to be the curator who functions as the gateway for linking and updating of information.

The Medical Record Institute's proposal in summary consists of:

1. no mandate for a Unique Patient Identifier

2. no change to the current practice of patient identification

3. a recommended DHHS mandate to the primary care physician to be the curator for linking and updating of patient information from multiple treatment locations

4. use of technology for linking and updating information from multiple locations without a Unique Patient Identifier.

II. Author/Proponent and Documentation

1. This method is proposed by Mr. C. Peter Waegemann, Executive Director, Medical Record Institute. Medical Record Institute's position paper and articles provide details about the method.

2. Medical Record Number is already a widely used identifier.

III. Compliance with ASTM Conceptual Characteristics

a) Functional Characteristics

***Accessible*:** Access to obtain the Identifier can be handled by provider organizations themselves.

***Assignable*:** Identifiers can be assigned by the provider organizations themselves.

Identifiable: The institutional MPI can support this function.

Verifiable: Organizations with computerized issue of Medical Record Numbers have the check-digit verification capability. Check-digit verification can be implemented with this method.

Mergeable: Duplicate medical record numbers are one of the problems facing the current institutional MPIs. Prevention of the issue of multiple medical record numbers has been a challenge and the merger of the respective records have been a persistent problem in healthcare organizations. Merging duplicate number can be done via cross-referencing.

Splittable: The instances of the same medical record number assigned to multiple individuals are fewer in relation to duplicate issues. However, the ability to split the same medical record number assigned to multiple individuals faces the same problems as merging duplicate numbers and records. This can be accomplished by issuing new number to one or all individuals that have the same number.

b) Linkage of Lifelong Health Record

The Medical Record Institute supports the retention of life long health record of only important information and not all patient care information.

Linkable: This function requires the Primary Care Physician to function as the curator to keep track of the location of care of an individual in order to link and support the electronic exchange of patient information.

Mappable: This function requires the Primary Care Physician to function as the curator to keep track of the location of care of an individual in order to create bidirectional linkage between the Medical Record Number with Provider Prefix and existing identifiers.

c) Patient Confidentiality and Security

Content Free: The proposed Identifier includes the Medical Record Number and provider ID within its content.

Controllable: Does not use encryption or decryption scheme to hide the identity of the individual

Healthcare Focused: Medical Record Number with a Provider Prefix is healthcare focused.

Secure: Does not use encryption nor requires a trusted authority to enforce a secure identifier

Disidentifiable: Does not use encryption or decryption scheme to hide the identity of

the individual

Public: Medical Record Number and Provider IDs are not public information and require security protection.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** This option is not based on industry standard.

Deployable: This option does not indicate any barriers and is compatible with technologies such as bar code readers, scanners, etc.

Usable: There is no inherent barrier to its use as a patient identifier.

e) Design Characteristics
The Department of Health and Human Services mandate to the primary care physician needs to be addressed by appropriate executive action. Protocol and procedures relating to the primary care physician's role including his or her power must be defined. A change in the choice of primary care physician by the patient and a change in the practice or affiliations of the primary care physician must be taken into account. Computer and communication system must be developed to facilitate the prompt and accurate exchange of information

Unique: The method does not recommend a unique identifier.

Repository-based: This method depends on the existing institutional Master Patient Index (MPI) data base.

Atomic: The proposed Identifier includes the provider ID within its content. It can be considered as a single data element.

Concise: The Medical Record Number with Provider Prefix is concise.

Unambiguous: Existing organization based Medical Record Numbers consists of numeric digits. Zeros and ones may present some ambiguity with letters "o" and "l" respectively.

Permanent: Patients will have multiple identifiers each issued by different organizations that delivered care. Within the same institution the identifier will be unique.

Centrally governed: The issue and maintenance of the ID are managed by the provider organization itself and does not require a central governing body.

Networked: The ID is issued and maintained within the same organization. There are no barriers to implementing the identifier over a network.

***Longevity*:** The scope of the Medical Record Number and its assignment to a Provider Prefix is limited to the issuing organization.

Retroactive: Does not apply. Medical Record Number is currently in use and not a new identifier proposal.

Universal: The scope of the organization-based Medical Record Number is not universal. It is intended only for patients visiting the organization. The Provider Prefix to the Medical Record Number is also organization based.

Incremental Implementation: Since this option is built upon the existing Medical Record Number it requires only the addition of the Provider Prefix which can be implemented incrementally.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: This option leaves the existing method of identification in tact except for the addition of the provider ID. Therefore, it will require minimum expenditure for implementation. However, its success and benefits depend on the ability of the Primary Care Provider who will function as the curator, and the computer's ability to exchange information without a unique identifier. It also depends on the feasibility of a DHHS mandate for the Primary Care Physician to function as the curator.

IV. Compliance with Unique Patient Identifier's Operational Characteristics and Readiness

Currently operational: Medical Record Number with a Provider Prefix is not currently operational. It is not a Unique Patient Identifier. Patients will receive multiple identifiers based on their choice of primary care physicians and provider organizations.

Existing infrastructure: Does not have existing administrative or technology infrastructure and the proposal does not address these requirements

Readiness of the required technology: The technology necessary to develop the infrastructure is available. The technology infrastructure including software applications, computer and communication systems must be developed to facilitate prompt and accurate exchange of information.

Timeliness: Medical Record Number with a Provider Prefix is not a Unique Patient Identifier. Medical Record Numbers are already in use. Therefore, addition of Provider Prefix should take relatively a short period of time. However, the provider prefix will require consensus on the choice of national provider identifier to be finalized first. In addition, an executive mandate by an appropriate authority must also be accomplished. Appropriate operating procedures, guidelines, technology and administrative infrastructures, etc. need to be created to handle situations involving

multiple organization specific medical record numbers and choice to change primary care physicians, patient's relocation, etc. The final solution may require a substantial amount of time to implement.

Adequacy of identification information to support identification functions: The organization specific MPIs do not have information on a patient's other record locations or care provided by other organizations. This will be dependent on the ability of the primary care physician to function as a curator to keep track of all locations of care, past and present.

V. Compliance with Unique Patient Identifier's Components Requirements

Identifier
Medical Record Number is organization specific. It is unique only within the organization that issued it. Medical Record Number with a Provider Prefix is not a Unique Patient Identifier. The Provider Number is subject to change based on the patient's choice of a different primary care physician, health plan or provider organization.

Identification Information
The patient's demographic information collected and maintained by provider organizations is accessible for use only within the same organization. The Primary Care Physician has the responsibility to track and maintain separately previous episodes of care and record locations.

Index
The Master Patient Index currently used by provider organizations are specific to respective organizations. They are not mappable to the same individual's identifier in another organization. The Primary Care Physician has the responsibility to track and maintain separately previous episodes of care and record locations.

Mechanism to protect, mask or encrypt the identifier
Encryption is not part of the proposal.

Technology Infrastructure
The scope of the technology infrastructure is limited to operation within the same provider organization. Its nation-wide scope is not addressed by the proposal.

Administrative Infrastructure
Scope of the administrative infrastructure is limited to operation within the same provider organization. Its nation-wide scope is not addressed by the proposal.

VI. Compliance with Basic Functions Criteria

Access to geographically-distributed information requires the patient identifier to expand beyond an institutional level. The existing institution-based medical record

numbers are adequate to manage the patient identification only within that institution. A robust identification method that can identify individuals uniquely across the nation and facilitate the linkage of their lifelong health record is the main objective of the Unique Patient Identifier. The institution-based Medical Record Number with provider prefix is not a Unique Patient Identifier. It does not fully comply with the Unique Patient Identifier's operational characteristics and component requirements. In the absence of these critical elements, the it lacks the ability to fulfill the basic functions discussed below.

Identification of individuals

Delivery of care functions: Medical Record Number with a provider prefix is not a Unique Patient Identifier that can support identification across multiple organizations. The positive identification of an individual is possible only within the organization that issued the identifier during the course of delivery of care.

Administrative functions: The identification for administrative functions required by practitioners, provider organizations, insurers, HMOs, federal health plan agencies, etc. is possible only within the organization that issued the identifier.

Identification of information

Coordination of multi-disciplinary care processes: The support for multi-disciplinary functions and coordination of care processes including, ordering of procedures, medications and tests and communication of results is possible only within the organization that issued the identifier.

Organization of patient information and medical record keeping: The support for manual medical record keeping and automated collection, storage and retrieval of information during the course of delivery of care is possible only within the organization that issued the identifier.

Manual and automated linkage of lifelong health records: The Medical Record Number lacks the ability to identify, organize and link information and records across multiple episodes of cares from multiple sites of care. This capability depends on the current primary care physician's ability to track, identify and link patient information from multiple organizations with multiple Medical Record Numbers and Provider IDs.

Aggregation of health information for analysis and research: The Medical Record Number lacks the ability to support the aggregation of health information across multiple episodes from multiple providers for research, planning and preventive measures. Once again, this capability depends on the current primary care physician's ability to track, identify and link patient information from multiple organizations with multiple Medical Record Numbers and Provider IDs.

Protection of privacy, confidentiality & security

Access Security: Access Security procedures are applicable only within the organization that issued the identifier. They are not addressed by the proposal.

Content-free Identifier: This option includes the primary care physician's Provider Identifier.

Mask/Hide/Encrypt/Protect/Disidentify: Does not use encryption

Improve health status and help reduce cost
The Medical Record Number with Provider Prefix is not a Unique Patent Identifier proposal. Its success is subject to the primary care physician's ability to track, identify and link patient information from multiple organizations with multiple Medical Record Numbers and Provider Identifiers and the development of the necessary technology solutions.

VII. Strengths and Weaknesses

Strengths:

1. Fully meets 17 of the 30 ASTM conceptual characteristics and partly meets 1

2. Uses existing identifier as part of the solution

3. Relatively easy to implement

4. Low cost of implementation

5. Does not require a Central Trusted Authority

6. Eliminates the effort, time and investment that will be required for developing and implementing a new identifier.

Weaknesses:

1. The Medical Record Number with a provider prefix is not a Unique Patient Identifier. Patient's ID will change when they change the primacy care physician.

2. Does not meet two of the five operational characteristics and a third is not adequately addressed

3. Only partially meets four of the six Unique Patient Identifier components' requirements and a fifth is not addressed

4. Only partially fulfills the basic functions of the Unique Patient Identifier

5. The existing medical record numbers have not been able to support exchange of information across institutional boundaries. System vendors are required to develop enterprise-wide MPI and cross indexes to link information from different institutions for the same patient which in turn led the industry in search for a Unique Patient Identifier.

6. Sophisticated computer tools and software have to be developed and introduced to address the exchange of information from multiple institutions with multiple identifiers for the same patient. This task has been an unfulfilled challenge for the industry.

7. Adequate protection must be provided to assure accurate matching and secure transmission of patient information.

8. Primary Care Physician's role has to be modified to include keeping track of the sites of care for individual patients.

9. The tracking of a patient's other sites of care or record locations depends on the ability of the patient's primary care physician.

10. A change in the choice of the Primary Care Physician by the patient or a change in the practice or affiliation by the Primary Care Physician can cause delay and difficulty in accessing information.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. Inclusion of missing identifier components and operational characteristics

2. Executive action for the designation of a Primary Care Physician as the curator to assume the responsibility for tracking the patient's sites of care and site-specific identifiers

3. Development of necessary communication technology and computer software to facilitate the exchange of information from multiple institutions with multiple identifiers for the same patient

4. Existing MPI errors such as duplicate Medical Record Numbers, incorrect and/or outdated information

5. Development of policies and procedures and implementation methodologies.

IX. Solutions to the Barriers:

1. Finalize the Provider Identifier choice and related issues.

2. Executive mandate relating to the Primary Care Physician's role as a curator for the linking and updating of information from multiple providers.

3.The clean-up of existing errors in the organizational MPIs

4. Development of the technology infrastructure including application software,

computer and communication issues to support the primary care physician's ability to perform the record location functions and exchange of information.

5. Development of implementation methodologies and policies and procedures.

10. CORBAMed Patient Identification Service (PIDS)

I. Description of the Option

CORBAMed is the healthcare division of the Object Management Group (OMG). OMG is an industry consortium for promoting the applications of Object Oriented Technologies. CORBA stands for Common Object Request Broker Architecture. It is the industry standard for object oriented interoperability among disparate computer systems. It provides notation for defining interfaces called OMG Interface Definition Language (IDL). CORBAMed is intended to be the object oriented interoperability standard for healthcare. The CORBAMed approach includes multiple levels of MPIs including departmental/service level, organizational level, enterprise level, etc. It uses an ID Domain Manager that manages the identification and correlation of patient demographic profile for searching and matching patient information. The CORBAMed specification currently does not include complex searches, such as searching for the location of a patient's previous sites of care or records. It requires the location of the site to communicate with its MPI. CORBAMed has issued a Request For Proposal for its Patient Identification Service and has received response from a consortium of vendors. The CORBAMed solution is not a proposal for a Unique Patient Identifier. It will, rather facilitate MPI level communication. It will search and match patient profiles for identifying patient and patient information. It will perform correlation of identifiers among ID domains in order to match the patient and patient information. According to CORBAMed representatives, both a Unique Patient Identifier and a central governing body with the knowledge of the various sites of a patient's record will help CORBAMed Patient Identification Service.

II. Author/Proponent and Documentation

1. CORBA has been in use for several years to implement interoperability among systems and handle integration needs. It is the industry standard for object-oriented technology.

2. OMG has published its Object Management Architecture for interoperability. CORBAMed's RFP specifications and responses to the RFP are available on the internet.

III. Compliance with ASTM Conceptual Characteristics

The CORBAMed PIDS is an object oriented software solution that searches and matches patient profiles for identifying patients and patient information. It is not a Unique Patient Identifier Proposal. Therefore, most of the ASTM Conceptual Characteristics relating to a UHID are not applicable to CORBAMed PIDS.

a) Functional Characteristics
***Accessible*:** Does not apply; not a Unique Patient Identifier proposal.

***Assignable*:** Does not apply; not a Unique Patient Identifier proposal.

Identifiable: Does not apply; not a Unique Patient Identifier proposal.

Verifiable: Does not apply; not a Unique Patient Identifier proposal.

Mergeable: Does not apply; not a Unique Patient Identifier proposal.

Splittable: Does not apply; not a Unique Patient Identifier proposal.

b) Linkage of Lifelong Health Record

Linkable: CORBAMed PIDS uses patient profiles and available identifiers to facilitate linkage of health records from multiple providers.

Mappable: Does not apply; not a Unique Patient Identifier proposal.

c) Patient Confidentiality and Security

Content Free: CORBAMed PIDS utilizes patient's demographic information and any available identifier for its searching and matching.

Controllable: Does not apply; not a Unique Patient Identifier proposal.

Healthcare Focused: CORBAMed PIDS is not a Unique Patient Identifier proposal, but it is healthcare focused.

Secure: Does not apply; not a Unique Patient Identifier proposal. The secure nature of the CORBAMed PIDS will depend on the design and development, yet to be performed.

Disidentifiable: CORBAMed PIDS is not a Unique Patient Identifier proposal. Encryption scheme to disidentify an individual is not part of the model.

Public: The patient identification information used by the CORBAMed PIDS for matching cannot be disclosed in public.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** CORBAMed PIDS is not a Unique Patient Identifier proposal.

Deployable: CORBAMed PIDS is not a Unique Patient Identifier proposal. The implementation requires the use of object-oriented technology.

Usable: Does not apply; not a Unique Patient Identifier proposal.

e) Design Characteristics

The CORBAMed approach uses OMA and OMG IDL as the technology architecture. It does not require an administrative infrastructure and its specifications do not address this. However, CORBAMed representatives point out a Central Trusted Authority with the knowledge of the patient record locations will help their process. These requirements and capabilities will be subject to the design and development that are yet to be performed.

Unique: Does not apply; not a Unique Patient Identifier proposal.

Repository-based: CORBAMed PIDS is not a repository-based Unique Patient Identifier..

Atomic: Does not apply; not a Unique Patient Identifier proposal.

Concise: Does not apply; not a Unique Patient Identifier proposal.

Unambiguous: Does not apply; not a Unique Patient Identifier proposal.

Permanent: Does not apply; not a Unique Patient Identifier proposal.

Centrally governed: CORBAMed PIDS proposal does not include a central governing body. However, a Central Trusted Authority would help the search process more efficient.

Networked: Deployable across networks

Longevity**:** Does not apply; not a Unique Patient Identifier proposal.

Retroactive: Does not apply; not a Unique Patient Identifier proposal.

Universal: Does not apply; not a Unique Patient Identifier proposal.

Incremental Implementation: Does not apply; not a Unique Patient Identifier proposal.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: The CORBAMed PIDS has the potential to link patient information distributed among multiple providers and enhance the health status of the nation. However, it is not a Unique Patient Identifier proposal and its cost-effectiveness will depend on its capability to fulfill all of the basic functions of a Unique Patient Identifier.

IV. Compliance with Unique Patient Identifier's Operational Characteristics

The CORBAMed Patient Identification Service's scope is limited to facilitating MPI level communication. It is not a Unique Patient Identifier proposal.

Currently operational: CORBAMed Patient Identification Service is not currently operational. It is in the RFP process.

Existing infrastructure: Does not have existing administrative or technology infrastructure.

Readiness of the required technology: The basic technology necessary to develop the infrastructure is ready and available.

Timeliness: CORBAMed has issued a Request For Proposal for its Patient Identification Service and has received response from a consortium of vendors. The method also requires the development of the software and communication solution and an implementation plan before nation-wide adoption. The project may require substantial amount of time.

Adequacy of information to support identification functions: CORBAMed PIDS will not maintain patient identification information.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
Not an Unique Patient Identifier proposal

Identification Information
Does not maintain patient identification information

Index
Does not maintain patient index

Mechanism to protect, mask or encrypt the identifier
Does not use encryption

Technology Infrastructure
CORBAMed Patient Identification Service is in RFP process to develop the technology.

Administrative Infrastructure
The Administrative Infrastructure is not included in the proposal, but indicates that both a Unique Patient Identifier and a central authority with the knowledge of record locations will help the CORBAMed Patient Identification Service.

VI. Compliance with Unique Patient Identifier's Basic

Functions Criteria

The main focus of the CORBAMed Patient Identification Service is to facilitate MPI to MPI communication. It is not a Unique Patient Identifier proposal. It does not meet all of the operational characteristics and component requirements of a Unique Patient Identifier. Therefore, its ability to perform the basic functions of the Unique Patient Identifier is significantly limited.

Identification of individuals

Delivery of care functions: The objective of the CORBAMed Patient Identification Service is MPI level communication. It is not a Unique Patient Identifier that can support the positive identification of an individual required during the course of delivery of care.

Administrative functions: CORBAMed Patient Identification Service is not a Unique Patient Identifier that can be used for patient identification during the course of delivery of care for administrative functions required by practitioners, insurers, HMOs, federal health plan agencies, etc.

Identification of information

Coordination of multi-disciplinary care processes: CORBAMed Patient Identification Service is not a Unique Patient Identifier that can facilitate the multi-disciplinary functions and coordination of care processes among multi-disciplinary team members.

Organization of patient information and medical record keeping: CORBAMed Patient Identification Service is not an identifier that can be used for medical record keeping or the organization of patient information.

Manual and automated linkage of lifelong health records: The CORBAMed Patient Identification Service is aimed at facilitating MPI level communication. Upon successful implementation, it will have the potential to search and match patients from multiple provider organizations. Together with the use of a Unique Patient Identifier and record locations, it can facilitate the linkage of information from different providers toward creating a lifelong health record.

Aggregation of health information for analysis and research: CORBAMed Patient Identification Service is not a Unique Patient Identifier for the aggregation of health information on the basis of diseases, treatments, outcomes, regions, etc. for research, planning and preventive measures.

Protection of privacy, confidentiality & security

Access Security: The CORBAMed Patient Identification Service's access security will depend on its final design and implementation.

Content-free Identifier: The CORBAMed Patient Identification Service is not a Unique Identifier proposal. It utilizes patient identification information for its

searching and matching.

Mask/Hide/Encrypt/Protect/Disidentify: The CORBAMed Patient Identification Service is not a Unique Identifier proposal.

Improve health status and help reduce cost
Upon successful implementation and subject to cooperation and participation by provider organizations, the CORBAMed Patient Identification Service will have the potential to search and match patients from multiple provider organizations. It will have a positive impact on the nation's health status. However, it is not a Unique Identifier proposal and its scope is limited to MPI level communication.

VII. Strengths and Weaknesses

Strengths:

1. Uses patient's demographic information and available identifier information to search and match patients, it does not mandate the implementation of a Unique Patient Identifier.

2. Eliminates the effort, time and investment that are required for developing and implementing a new identifier.

Weaknesses:

1. Not a Unique Patient Identifier and does not meet the ASTM conceptual characteristics of UHID (meets only 3 of the 30 requirements).

2. Does not meet three of the five Unique Patient Identifier's operational characteristics and only partially meets the remaining two characteristics.

3. Does not meet any of the Unique Patient Identifier Components' requirements.

4. Does not meet most of the Unique Patient Identifier Basic Functions requirements. The focus is mainly on MPI to MPI communication.

5. The search is limited to participating locations.

6. Does not perform search for sites of care/record location.

7. Requires:

    a) prior knowledge of record location and sufficient identification information. More the availability of patient identification information the greater the success.

    b) provider organization's participation in the CORBAMed project and

their authorization for searching the patient, patient identifier and patient information by another computer system.

c) adequate security arrangements for searching and exchanging patient information.

d) development and implementation of powerful and reliable searching and matching algorithms.

8. The probabilistic matching does not assure 100% result. Discrepancies may require human intervention for resolution.

9. Currently, the CORBAMed PIDS is in the RFP process and for most part remains as a concept. Its fruition will depend upon significant planning, preparation, specification, design and development.

10. Untested - implementing a brand new system nationwide that has not been proven in healthcare industry has inherent risk for its success.

11. The method requires the development of an implementation plan and creation of necessary operating procedures.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. CORBAMed PIDS is in the RFP process. Its development, testing, nation-wide deployment and user acceptance are yet to be accomplished.

2. CORBAMed PIDS is a software solution for MPI level searching and matching of patients with available information including Unique Patient Identifiers. It is not a Unique Patient Identifier proposal. Therefore, it lacks the ability to assume the role of a Unique Patient Identifier and perform its functions.

3. Timely development of necessary communication technology and computer software.

IX. Solutions to the Barriers:

The CORBAMed Patient Identification Service is not a Unique Patient Identifier Proposal. It must include a Unique Patient Identifier solution in addition to its MPI to MPI communication capability. The solutions to barriers will include:

1. Inclusion of the missing Unique Patient Identifier's operational characteristics

2. Inclusion of the missing Unique Patient Identifier's components

3. Inclusion of the missing Unique Patient Identifier's basic functions requirements

4) Development of the CORBAMed PIDS software, implementation of standards, technology, communication protocols, etc.

11. HL7 Master Patient Index Mediator

I. Description of the Option

The HL7 mediation is a software transaction process transmitted to search and locate patients in other MPIs. The software device will send demographic characteristics using HL7 transaction standards to locate and match demographic information in the receiving MPI. The greater the number of demographic characteristics the greater is the matching success. HL7 has organized a MPI Special Interests Group (SIG) to develop this concept further and implement the solution. The SIG's goal is to recommend improvements or extensions to existing HL7 specifications which support mediation among local MPI's (Master Patient Indices). The specifications will describe processes by which an individual can be uniquely identified and coordinated across multiple internal and external systems as well as existing and future systems. Although HL7 does not require a Unique Patient Identifier for mediation, it will be greatly benefitted by it.

Mr. James M. Gabler, Co-chair of the HL7 MPI Special Interest Group points out that multiple identifiers exist and should continue to be used. He believes that a system (provider organization) must be able to assign a system specific unique ID and the role of internal and external ID should be kept separate. HL7's MPI Mediation initiative is to support the on-going facilitation for the multiplicity of identifiers associated with each person through cross-referencing (mediation). It will create a seamless patient population across the participating patient registration systems within a multi-system enterprise.

II. Author/Proponent and Documentation

1. HL7 transaction standards are already used by the industry to update and maintain local MPIs. The proposed improvement adds the use of object-oriented technology to facilitate mediation among both internal and external MPIs.

2. HL7 is an ANSI accredited Standards Developing Organization. HL7 Transaction Standards have been published. The document relating to the MPI Mediator's scope and objectives is used for this analysis.

III. Compliance with ASTM Conceptual Characteristics

The HL7 Mediation is an object-oriented software solution to identify patients and patient information across multiple internal and external systems. It is not a Unique Patient Identifier Proposal. Therefore, most of the ASTM Conceptual Characteristics relating to a UHID are not applicable to HL7 Mediation.

a) Functional Characteristics

***Accessible*:** Does not apply; not a Unique Patient Identifier proposal.

***Assignable*:** Does not apply; not a Unique Patient Identifier proposal.

Identifiable: Does not apply; not a Unique Patient Identifier proposal. Provider specific internal identifier and MPI will be referenced for identification.

Verifiable: Does not apply; not a Unique Patient Identifier proposal.

Mergeable: Does not apply; not a Unique Patient Identifier proposal.

Splittable: Does not apply; not a Unique Patient Identifier proposal.

b) Linkage of Lifelong Health Record

Linkable: HL7 Mediation uses patient profiles and available identifiers to facilitate linkage of health records from multiple providers.

Mappable: Does not apply; not a Unique Patient Identifier proposal.

c) Patient Confidentiality and Security

Content Free: HL7 MPI Mediator utilizes patient's demographic information and available identifier for its searching and matching.

Controllable: Does not apply; not a Unique Patient Identifier proposal.

Healthcare Focused: The HL7 MPI Mediator is intended for the use of healthcare.

Secure: Does not apply; not a Unique Patient Identifier proposal.

Disidentifiable: Encryption scheme to disidentify an individual is not part of the model.

Public: The patient information used by the HL7 MPI Mediator for matching is not public information.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** HL7 MPI Mediator is not a Unique Patient Identifier proposal.

Deployable: HL7 MPI Mediator is not a Unique Patient Identifier proposal. Object-oriented technology will be used for its implementation.

Usable: Does not apply; not a Unique Patient Identifier proposal.

e) Design Characteristics

The HL7 is planning to use object-oriented technology for designing and developing its MPI Mediator. It does not require an administrative infrastructure and its specifications do not address this. However, HL7 representatives point out a Unique Patient Identifier with appropriate Central Trusted Authority and knowledge of the patient record locations will help their process.

Unique: Does not apply; not a Unique Patient Identifier proposal.

Repository-based: It is not repository-based. This is, however, not a Unique Patient Identifier proposal.

Atomic: Does not apply; not a Unique Patient Identifier proposal.

Concise: Does not apply; not a Unique Patient Identifier proposal.

Unambiguous: Does not apply; not a Unique Patient Identifier proposal.

Permanent: Does not apply; not a Unique Patient Identifier proposal.

Centrally governed: HL7 MPI Mediator does not include a central governing body. A Central Trusted Authority with the knowledge of the patient record locations will help the process.

Networked: HL7 MPI Mediator is deployable across networks.

Longevity**:** Does not apply; not a Unique Patient Identifier proposal.

Retroactive: Does not apply; not a Unique Patient Identifier proposal.

Universal: Does not apply; not a Unique Patient Identifier proposal.

Incremental Implementation: Does not apply, not a Unique Patient Identifier proposal.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: The HL7 Mediation has the potential to link patient information distributed among multiple providers and enhance the health status of the nation. However, it is not a Unique Patient Identifier proposal and its cost-effectiveness depends on its capability to fulfill all of the basic functions of a Unique Patient Identifier.

IV. Compliance with Operational Characteristics and Readiness

Currently operational: The HL7 MPI Mediation is not a Unique Identifier. It is not currently operational.

Existing infrastructure: The HL7 MPI Mediation is not a Unique Patient Identifier proposal. Its objective is to improve existing transaction standards to facilitate communication among MPIs from different organizations.

Readiness of the required technology: The basic technology necessary to develop the MPI Mediation is ready and available.

Timeliness: The HL7 MPI Mediation Special Interest Group is a new initiative in a planning stage. The development of specifications and the final solution may require substantial amount of time.

Adequacy of information to support identification functions: HL7 MPI Mediator is not a Unique Patient Identifier and it will not maintain patient identification information.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
The HL7 MPI Mediator is not a Unique Patient Identifier

Identification Information
The HL7 Mediation is not a Unique Patient Identifier and it does not maintain a patient identification data base.

Index
The HL7 Mediation is not an Unique Patient Identifier and it does not maintain a patient index.

Mechanism to protect, mask or encrypt the identifier
Does not use encryption

Technology Infrastructure
The HL7 Mediation is not an Unique Patient Identifier. Its specifications and technology development are at a planning stage.

Administrative Infrastructure
The HL7 Mediation is not a Unique Patient Identifier. Administrative Infrastructure is not addressed. HL7 representatives indicate that both the availability of a Unique Patient Identifier and the use of a Central Trusted Authority with the knowledge of record locations will help the HL7 Mediation process.

VI. Compliance with Basic Functions Criteria

The main focus of the HL7 MPI Mediation is to search and locate patients in other MPIs through the use of software transactions. It is not a Unique Patient Identifier proposal. It does not meet all of the operational characteristics and component requirements of the Unique Patient Identifier. Therefore, its ability to perform the basic functions of the Unique Patient Identifier is significantly limited.

Identification of individuals

Delivery of care functions: The objective of the HL7 Mediation is MPI level communication. It is not a Unique Patient Identifier that can support the positive identification of an individual required during the course of delivery of care.

Administrative functions: HL7 Mediation is not a Unique Patient Identifier that can be used for patient identification during the course of delivery of care for administrative functions required by practitioners, insurers, HMOs, federal health plan agencies, etc.

Identification of information

Coordination of multi-disciplinary care processes: HL7 Mediation is not a Unique Patient Identifier that can facilitate the multi-disciplinary functions and coordination of care processes among multi-disciplinary team members.

Organization of patient information and medical record keeping: HL7 Mediation is not a Unique Patient Identifier that can be used for medical record keeping or organization of patient information.

Manual and automated linkage of lifelong health records: The HL7 Mediation is aimed at facilitating MPI level communication. Upon successful implementation, it will have the potential to search and match patients from multiple provider organizations. Together with the use of a Unique Patient Identifier and record locations, it can facilitate the linkage of information from different providers to create a lifelong health record.

Aggregation of health information for analysis and research: HL7 Mediation is not a Unique Patient Identifier that can be used for the aggregation of health information on the basis of diseases, treatments, outcomes, regions, etc. for research, planning and preventive measures.

Protection of privacy, confidentiality & security

Access Security: The HL7 Mediation's access security will depend on its final design and implementation.

Content-free Identifier: The HL7 Mediation is not a Unique Patient Identifier proposal. It utilizes patient identification information for searching and matching.

Mask/Hide/Encrypt/Protect/Disidentify: The HL7 Mediation is not a Unique

Identifier proposal. It does not include encryption.

Improve health status and help reduce cost

Upon successful implementation and subject to cooperation and participation by provider organizations, the HL7 Mediation will have the potential to search and match patients from multiple provider organizations. It will have a positive impact on the nation's health status. However, it is not a Unique Identifier proposal and its scope is limited to MPI level communication.

VII. Strengths and Weaknesses

Strengths:

1. Uses patient's demographic information and available identifiers to search and match patients and does not mandate the use of a Unique Patient Identifier, although it will be helped by it.

2. Eliminates the effort, time and investment that will be required for developing and implementing a new identifier.

Weaknesses:

1. Not a Unique Patient Identifier and does not meet the ASTM conceptual characteristics of UHID.(meets only 3 of the 30 requirements)

2. Does not meet the five Unique Patient Identifier's operational characteristics

3. Does not meet any of the Unique Patient Identifier Components' requirements

4. Does not meet most of the Unique Patient Identifier's basic functional requirements. The focus is mainly on cross-referencing existing internal and external identifiers

5. The search will be limited to participating locations.

6. Does not perform search for sites of care/record locations.

7. Requires:

    a) prior knowledge of record location and sufficient identification information. The more the availability of patient identification information, the greater the success.

    b) provider organization's participation in the HL7 Mediation and authorization for searching for the patient, patient identifier and patient information by another computer system.

c) adequate security arrangements for searching and exchanging patient information

d) development and implementation of powerful and reliable searching and matching algorithms.

8. The probabilistic matching utilized by software approaches does not assure 100% result. Discrepancies may require human intervention for resolution

9. Currently, the HL7 Mediation is in the preliminary stage and its fruition depends on significant planning, specification, design and development.

10. The method requires development of an implementation plan and creation of necessary operating procedures, etc.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. Failure to meet all of the Unique Patient Identifier's operational characteristics

2. Failure to meet all of the Unique Patient Identifier's component requirements

3. Inability to fulfill all of the basic functions of a Unique Patient Identifier

4. Development of the necessary communication technology and computer software to facilitate the exchange of information from multiple institutions with multiple identifiers for the same patient

5. Timeliness.

IX. Solutions to the Barriers:

The HL7 Mediation is not a Unique Patient Identifier Proposal. It must include a Unique Patient Identifier solution in addition to its software matching process. The solutions to barriers will include:

1. Inclusion of the missing Unique Patient Identifier's operational characteristics

2. Inclusion of the missing Unique Patient Identifier's components

3. Inclusion of the missing Unique Patient Identifier's basic functions requirements

4. Development of the HL7 Mediation software, implementation of standards, technology, communication protocols, etc.

12. FHOP's Core Data Element-Based Patient Identification

I. Description of the Options

The University of California, San Francisco Family Health Outcomes Project (FHOP) recommends the use of standard data sets for the identification of patient information. FHOP is part of the Department of Family and Community Medicine and is affiliated with the Institute of Health Policy Studies in California. FHOP has opted for data standardization and unique client identification instead of establishing a unique client ID. FHOP's identifying data elements consist of two sets namely Core Data Elements and Confirmatory Data Elements. The Core Data Elements consist of the following five (5) data items:

1. Birth Name
2. Birth Date
3. Birth Place
4. Mother's First Name
5. Gender

The Confirmatory Data Elements consist of the following seven (7) data items:

1. Social Security Number
2. Other Client Number
3. Father's Name
4. Mother's Maiden Name
5. Current Name/Client Alias/Nickname
6. County of Client's Residence
7. Zip of Client's Residence

The FHOP approach uses object oriented software technology and a method known as blocking technique. The blocking technique is used to determine the relative weighting of each of the common data elements and their sequence. From the resulting data set in their weighted order an alphanumeric string value is derived. This value is used to detect and link duplicate records in pilot projects which yielded impressive results. FHOP points out that the alphanumeric value based on the common core data elements can be used as a Common Patient Identifier. The Common Patient Identifier value can be destroyed after linkage. It will then serve as a Virtual Identifier. An object-oriented software matching algorithm is used for a probabilistic matching. The FHOP proposal is aimed at facilitating database linkage among the various centers of care with data standardization. They do not replace the institution specific identifiers that are currently used at the various branches of the statewide health services for managing the patient encounter and record keeping.

II. Author/Proponent and Documentation

1. The University of California, San Francisco Family Health Outcomes Project (FHOP) is the proponent of this method. .

2. Data Element Specification document and Dr. Geraldine Olivia's description of the methodology are the documents available for this analysis.

III. Compliance with ASTM Conceptual Characteristics

a) Functional Characteristics

***Accessible*:** Does not apply; the method uses patients' demographic information instead of a Unique Patient Identifier.

***Assignable*:** Does not apply; the method uses patients' demographic information instead of a Unique Patient Identifier.

Identifiable: FHOP uses a set of five Common Core Data Elements and seven Confirmatory Data Elements.

Verifiable: Not applicable; FHOP's Core Data Element-based Patient Identification is not a Unique Patient Identifier proposal.

Mergeable: FHOP's Core Data Element-based Patient Identification is not a Unique Patient Identifier proposal. It uses a set of five Common Core Data Elements and seven Confirmatory Data Elements. Pilot studies have shown its ability to identify duplicate records.

Splittable: Not applicable; FHOP's Core Data Element-based Patient Identification is not a Unique Patient Identifier proposal.

b) Linkage of Lifelong Health Record

Linkable: Pilot studies have shown its ability to identify duplicate records.

Mappable: FHOP's Core Data Element-based Patient Identification can map patient's existing identifiers.

c) Patient Confidentiality and Security

Content Free: FHOP's approach utilizes a set of patient's personal identification information.

Controllable: FHOP's proposal does not include encryption.

Healthcare Focused: The FHOP's Common Core Data Element and Confirmatory

Data Elements are healthcare focused.

Secure: FHOP's proposal does not include encryption.

Disidentifiable: FHOP's proposal does not include encryption for disidentification.

Public: The patient information used by the FHOP approach cannot be disclosed in public.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** FHOP's Core Data Element-based identification is not based on industry standard.

Deployable: FHOP's Core Data Element-based Patient Identification uses the object-oriented software technology.

Usable: The five Common Core Data Elements and seven Confirmatory Data Elements will be difficult to process manually on a routine basis. It requires the use of a computer program to process the identification.

e) Design Characteristics

The FHOP's approach uses object-oriented technology for identifying and matching patient information. It does not address the administrative infrastructure.

Unique: The Common Core Data Elements and Confirmatory Data Elements support the unique identification of individuals.

Repository-based: FHOP's Core Data Element-based Patient Identification is not a Unique Patient Identifier supported by a repository.

Atomic: FHOP's Core Data Element-based Patient Identifier is not atomic.

Concise: FHOP's Core Data Element-based Patient Identifier is not concise.

Unambiguous: Not applicable FHOP's Core Data Element-based Patient Identification is not a Unique Patient Identifier.

Permanent: Not applicable FHOP's Core Data Element-based Patient Identification is not a Unique Patient Identifier.

Centrally governed: FHOP's approach does not include a central governing body.

Networked: Applications based on object-oriented technology can be deployed over networks.

***Longevity*:** Does not apply; not a Unique Patient Identifier.

Retroactive: Does not apply; not a Unique Patient Identifier proposal.

Universal: Does not apply; not a Unique Patient Identifier proposal.

Incremental Implementation: Can be implemented incrementally.

f) Reduction of Cost and Enhanced Health Status

The FHOP Common Core Data Elements have the potential to link duplicate patient records. It does not replace the existing site (provider) specific patient identifier and does not address all of the basic functions of a Unique Patient Identifier.

Cost-effectiveness: This method uses object oriented computer technology to process the actual demographic information for identification. It does not replace the existing patient identifier. It is currently used for the management of clinical data bases. Cost effectiveness depends on this option's capability to fulfill all of the basic functions of a Unique Patient Identifier.

IV. Compliance with Operational Characteristics and Readiness

Currently operational: Not operational as a Unique Identifier. FHOP's Core Data Elements and Confirmatory Data Elements have been field tested in three pilot counties in California for data base applications.

Existing infrastructure: Infrastructure for nation-wide application is not addressed.

Readiness of the required technology: FHOP uses object oriented software algorithm for its local application. The basic technology necessary to develop the infrastructure is ready and available.

Timeliness: Use of patients' actual demographic information instead of an identifier across the nation and development of appropriate technology infrastructure are expected to require enormous amount of time, resource and effort.

Adequacy of information to support identification functions: FHOP's Core Data Element-based Patient Identification uses a set of five Common Core Data Elements and seven Confirmatory Data Elements. They do not include provider information or record locations relating to previous episodes of care.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
Not a Unique Patient Identifier. FHOP's method uses the actual identification data elements of the patients instead of an identifier.

Identification Information
Not a Unique Patient Identifier. FHOP's method uses a set of five Common Core Data Elements and seven Confirmatory Data Elements. They do not include provider information or record locations relating to previous episodes of care.

Index
FHOP's method uses the actual identification data elements of the patients instead of an identifier. It does not use an Index.

Mechanism to protect, mask or encrypt the identifier
Does not use encryption

Technology Infrastructure
FHOP uses object oriented software developed locally. Nation-wide application is not addressed.

Administrative Infrastructure
Nation-wide administrative infrastructure is not addressed.

VI. Compliance with Basic Functions Criteria

FHOP's method is not a Unique Patient Identifier proposal. It makes use of the actual identification data elements of the patients instead of an identifier. It does not meet all of the operational characteristics and component requirements of the Unique Patient Identifier. Therefore, its ability to perform the basic functions of the Unique Patient Identifier is significantly limited.

Identification of individuals
Delivery of care functions: FHOP's method does not use a Unique Patient Identifier. It requires the use of actual data elements. Transcription errors, spelling mistakes and other discrepancies can interfere with the identification process. Manual verification and use may prove to be cumbersome, time consuming and error prone during the delivery of care.

Administrative functions: FHOP's method requires the use of actual data elements. Transcription errors, spelling mistakes and other content discrepancies may interfere with the identification process. Manual verification and use may prove to be cumbersome, time consuming and error prone for administrative processes both during and after the delivery of care.

Identification of information

Coordination of multi-disciplinary care processes: FHOP's method requires the use of actual data elements to facilitate the multi-disciplinary functions and coordination of care processes among multi-disciplinary team members. However, transcription errors, spelling mistakes and other content discrepancies may interfere with the identification process. Manual verification and use may prove to be cumbersome, time consuming and error prone for administrative processes both during and after the delivery of care.

Organization of patient information and medical record keeping: FHOP's method requires the use of actual data elements. Transcription errors, spelling mistakes and other content discrepancies may interfere with the identification process. Manual verification and use may prove to be cumbersome, time consuming and error prone for the maintenance of medical record and information management.

Manual and automated linkage of lifelong health records: FHOP's method requires the use of actual data elements. Transcription errors, spelling mistakes and other content discrepancies may interfere with the identification process while linking information from multiple sites of care and different providers. Manual verification and use may prove to be cumbersome, time consuming and error prone for administrative processes both during and after the delivery of care.

Aggregation of health information for analysis and research: FHOP's method requires the use of actual data elements. Transcription errors, spelling mistakes and other content discrepancies may interfere with the identification process while aggregating information from multiple sites of care and different providers.

Protection of privacy, confidentiality & security

Access Security: The Access Security and the authentication procedures needed to access the patient care information for the nation-wide application is not addressed.

Content-free Identifier: FHOP's method makes use of the actual identification data elements of the patients instead of an identifier.

Mask/Hide/Encrypt/Protect/Disidentify: Does not include encryption

Improve health status and help reduce cost

Since the FHOP's method makes use of the actual identification data elements of the patients instead of an identifier, it may prove to be an expensive and time consuming option.

VII. Strengths and Weaknesses

Strengths:

1. Uses a common set of data elements from which an alphanumeric value can be derived to serve as a Patient Identifier or a Temporary/Virtual Identifier

2. Uses a set of data elements that patients are familiar with

3. Eliminates the effort, time and investment that will be required for developing and implementing a new identifier.

Weaknesses:

1. Not a Unique Patient Identifier and does not meet ASTM requirements (meets only 8 of the 30 requirements)

2. Does not meet three (3) of the five (5) Unique Patient Identifier's operational characteristics and only partially meets the remaining two (2)

3. Does not meet four (4) of the six Unique Patient Identifier Component requirements and only partially meets the remaining two (2)

4. Only partially fulfills the Unique Patient Identifier's basic functional requirements

5. Does not replace existing identifiers, but is used in addition to existing identifier

6. Use of Common Core Data Elements in combination with seven additional Confirmatory Data Elements for identification, verification, registration and patient care communication and other day-today activities may become complex, time consuming and burdensome

7. FHOP approach uses patient data and therefore, not content free.

8. The use of patient's personal information for identification instead of a content free identifier has inherent risk for violation of privacy.

9. Searching and accurately matching 5 to 12 data elements instead of a single identifier present complexity even with computer.

10. The alphanumeric value derived for use as a Common Patient Identifier or a temporary Virtual Identifier requires the use of weighting and probabilistic matching algorithms which are too complex for manual use.

11. The approach relies on patient's accurate supply of Data Elements every time.

12. Inconsistent spellings, mispronunciation and typographical errors may alter the value of both the Common Patient Identifier and Virtual Identifier values.

13. Pilot projects by FHOP were designed to identify, link and eliminate duplicate records from databases. The method's applicability to perform all of the basic functions of a Unique Patient Identifier has not been established.

14. Nation-wide use which includes accessing independent organizations and

searching, matching and exchanging information has not been included in the proposal.

15. Nation-wide application requires:

a) prior knowledge of record location and sufficient identification information

b) provider organization's participation in the FHOP's Core Data Element-based Patient Identification process and authorization for searching for the patient, patient identifier and patient information by another computer system

c) adequate security arrangements for searching and exchanging patient information

d) development and implementation of a powerful and reliable searching and matching algorithms.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. Ability to fulfill all of the basic functions of a Unique Patient Identifier functions

2. Development of necessary communication technology and computer software and tools to facilitate access and the exchange of information from multiple institutions

3. Both the Common Core Data Elements and Confirmatory Data Elements have patient's personal information with potential for violation of patient's privacy.

4. Adequate protection must be provided to assure accurate matching and secure transmission of patient information.

5. Cost-effectiveness

6. Timeliness.

IX. Solutions to the Barriers:

The FHOP Core Data Element-based Identification is not a Unique Patient Identifier Proposal. It must include a Unique Patient Identifier solution in addition to its core and confirmatory data elements. The solutions to barriers includes:

1. Inclusion of the missing Unique Patient Identifier's operational characteristics

2. Inclusion of the missing Unique Patient Identifier's components

3. Inclusion of the missing Unique Patient Identifier's basic functions requirements

4. The ability to fully meet all of the basic functions of the Unique Patient Identifier

5. Development of the technology infrastructure including application software, computer and communication protocols for the nation-wide use

6. Development of administrative infrastructure to address the nation-wide use

7. Development of implementation methodologies, policies and procedures.

13. Directory Service

I. Description of the Option

William L. McMullen from Mitertek recommends the use of Directory Service instead of a Unique Patient Identifier to link patient information. The Directory Service would use existing patient identifiers of legacy systems in a manner to provide linkages to records of individuals across systems. The directory service system uses patient characteristics such as social characteristics (name, SSN, address, driver license etc.) human characteristics (finger print, retina scan etc.) and other groupings such as sex, race, DOB, etc. The directory service would reconcile interactively and heuristically the proper association of the patient identification data at the current point of care with any one of the other prior points of care. This step would be supported by automated capabilities that would facilitate locating the other patient records for which a record linkage is valid. The current point of care location would then be linked with any of the other selected point of care locations by electronically exchanging their network addresses.

Mr. McMullen's method is implemented in the state of Georgia to manage access to mental health patient information. Although he is not currently involved in this project, he strongly believes that the Directory Service model can be used instead of implementing a nation-wide Unique Patient Identification System. He points out that his original Directory Service concept needs to be updated. His current recommendation consists of the internet-based Netscape Catalogue Service instead of the Directory Service. He feels a subscription based funding model similar to the internet services can be utilized and the expense shared by participating organizations. This will be less expensive than implementing a Unique Patient Identifier nation-wide.

II. Author/Proponent and Documentation

1. Mr. McMullen's Directory Service is being used by the state of Georgia to manage access to mental health patient information.

2. The method is being recommended by Mr. William McMullen of Mitertek Corporation. His past document outlining his original method is the only document available for review.

III. Compliance with ASTM Conceptual Characteristics

The Directory Service utilizes patient characteristics information such as name, SSN, address, driver license, sex, race, DOB, etc. to reconcile interactively and heuristically the proper association of the patient identification data at the current point of care with any one of the other prior points of care. It is not a Unique Patient Identifier proposal. Therefore, most of the ASTM Conceptual Characteristics are not applicable to the Directory Service.

a) Functional Characteristics

***Accessible*:** Does not apply, not a Unique Patient Identifier proposal.

***Assignable*:** Does not apply, not a Unique Patient Identifier proposal.

Identifiable: Does not apply, not a Unique Patient Identifier proposal.

Verifiable: Does not apply, not a Unique Patient Identifier proposal.

Mergeable: Does not apply, not a Unique Patient Identifier proposal.

Splittable: Does not apply, not a Unique Patient Identifier proposal. .

b) Linkage of Lifelong Health Record

Linkable: The Directory Service uses patient profiles and available identifiers to facilitate linkage of health records from multiple providers.

Mappable: Does not apply, not a Unique Patient Identifier proposal.

c) Patient Confidentiality and Security

Content Free: The searching and matching performed by the Directory Service utilize patient's demographic information and available identifiers

Controllable: Does not use encryption

Healthcare Focused: The Directory Service proposed by Mr. McMullen is healthcare-focused.

Secure: Encryption is not included in the proposal.

Disidentifiable: Encryption scheme to disidentify an individual is not part of the model.

Public: The patient demographic information used by the Directory Service for matching cannot be disclosed in public.

d) Compatibility with Standards and Technology

***Based on Industry Standards*:** Directory Service is not a Unique Patient Identifier proposal.

Deployable: The Directory Service can be implemented with the existing technology. However, it is not a Unique Patient Identifier proposal.

Usable: Directory Service is not a Unique Patient Identifier proposal.

e) Design Characteristics

For nation-wide use the Directory Service model will need both a technology and administrative infrastructure. The current proposal does not include the administrative infrastructure issue. The Directory Service concept needs to be developed further. These capabilities will be subject to the appropriate specification, design and development that are yet to be organized.

Unique: Directory Service is not a Unique Patient Identifier proposal. It uses patient's social and personal characteristics for searching and matching.

Repository-based: Directory Service is not a Unique Patient Identifier proposal. It is not repository-based.

Atomic: Directory Service is not a Unique Patient Identifier proposal.

Concise: Directory Service is not a Unique Patient Identifier proposal.

Unambiguous: Directory Service is not a Unique Patient Identifier proposal.

Permanent: Directory Service is not a Unique Patient Identifier proposal.

Centrally governed: Directory Service is not a Unique Patient Identifier proposal. A Central Trusted Authority with the knowledge of the location of patient information will help the process.

Networked: Directory Service is based on telecommunication (modem) and networks.

Longevity**:** Directory Service is not a Unique Patient Identifier proposal.

Retroactive: Directory Service is not a Unique Patient Identifier proposal.

Universal: Directory Service is not a Unique Patient Identifier proposal.

Incremental Implementation: Does not apply. Directory Service is not a Unique Patient Identifier proposal.

f) Reduction of Cost and Enhanced Health Status

Cost-effectiveness: The Directory Service has the potential to access patient information distributed among multiple provider organizations that participate in the Directory Service. However, it is not a Unique Patient Identifier proposal and does not address all the basic functions of a Unique Patient Identifier.

IV. Compliance with Operational Characteristics and Readiness

Currently operational: The Directory Service is not a Unique Patient Identifier. It is used on a limited basis for access to mental health patient records in the state of Georgia. It is not currently operational as a Unique Patient Identifier.

Existing infrastructure: Both the administrative and technology infrastructures are not in existence for nation wide use.

Readiness of the required technology: The basic technology necessary to develop the infrastructure is ready and available. However, the application software and communication systems are yet to be developed.

Timeliness: The Directory Service is a new initiative for healthcare. The development of specifications and the final solution may require substantial amount of time.

Adequacy of information to support identification functions: The Directory Service is not a Unique Patient Identifier and it does not maintain patient identification information.

V. Compliance with Unique Patient Identifier Components Requirements

Identifier
The Directory Service is not a Unique Patient Identifier.

Identification Information
The Directory Service does not maintain a patient identification data base.

Index
The Directory Service is not a Unique Patient Identifier and it does not maintain a patient index.

Mechanism to protect, mask or encrypt the identifier
Does not use encryption

Technology Infrastructure
The Directory Service is not a Unique Patient Identifier. The necessary specifications, design and technology development are yet to be planned.

Administrative Infrastructure
The Directory Service is not a Unique Patient Identifier. Administrative Infrastructure is not addressed.

VI. Compliance with Basic Functions Criteria

The main focus of the Directory Service is to use patient's personal identification information and existing identifiers to provide linkage of records of individuals across systems. It is not a Unique Patient Identifier proposal. It does not meet all of the operational characteristics and component requirements of the Unique Patient Identifier. Therefore, its ability to perform the basic functions of the Unique Patient Identifier is significantly limited.

Identification of individuals

Delivery of care functions: The objective of the Directory Service to provide linkage of records across systems using existing identifiers and personal identification information. It does not support the positive identification of an individual required during the course of delivery of care.

Administrative functions: Does not support patient identification during the course of delivery of care for administrative functions required by practitioners, insurers, HMOs, federal health plan agencies, etc.

Identification of information

Coordination of multi-disciplinary care processes: Directory Service is not a Unique Patient Identifier that can facilitate the multi-disciplinary functions and coordination of care processes among multi-disciplinary team members.

Organization of patient information and medical record keeping: Directory Service is not an identifier that can be used for medical record keeping or the organization of patient information.

Manual and automated linkage of lifelong health records: Upon successful implementation, the Directory Service will have the potential to search and match patients from multiple provider organizations. Together with the use of a Unique Patient Identifier and record locations, it can facilitate the linkage of information from different providers toward creating a lifelong health record.

Aggregation of health information for analysis and research: Directory Service is not a Unique Patient Identifier for the aggregation of health information on the basis of diseases, treatments, outcomes, regions, etc. for research, planning and preventive measures.

Protection of privacy, confidentiality & security

Access Security: The access security of the Directory Service will depend on its final design and implementation.

Content-free Identifier: The Directory Service utilizes patient identification information for searching and matching.

Mask/Hide/Encrypt/Protect/Disidentify: The Directory Service does not include encryption.

Improve health status and help reduce cost Upon successful implementation and subject to cooperation and participation by provider organizations, the Directory Service will have the potential to search and match patients from multiple provider organizations. It will have a positive impact on the nation's health status. However, it is not a Unique Identifier proposal and its scope is limited to record linkage.

VII. Strengths and Weaknesses

Strengths:

1. Uses patient's social and human characteristics and does not require the implementation of a Unique Patient Identifier

2. Eliminates the effort, time and investment that will be required for developing and implementing a new identifier

Weaknesses:

1. Not a Unique Patient Identifier and does not meet the ASTM conceptual characteristics of UHID (meets only 3 of the 30 requirements)

2. Does not meet the five Unique Patient Identifier's operational characteristics

3. Does not meet any of the Unique Patient Identifier Component requirements

4. Does not meet most of the Unique Patient Identifier's basic functional requirements. The focus is mainly on searching and matching patient record with the use of available identification information and identifiers

5. The search is limited to participating locations.

6. Requires:

    a) prior knowledge of record location and sufficient identification information. The more the availability of patient identification information the greater the success

    b) provider organization's participation in the Directory Service and permission for searching for the patient, patient identifier, patient information by another computer system

    c) adequate security arrangements for searching and exchanging patient information

    d) development and implementation of a powerful and reliable searching and matching algorithms

7. The probabilistic matching utilized by software approaches does not assure 100% result. Discrepancies may require human intervention for resolution.

8. Currently, the Directory Service is in the preliminary stage and its fruition depends on significant planning, specification, design and development.

9. The method requires the development of an implementation plan and creation of necessary operating procedures, etc.

VIII. Potential Barriers & Challenges to Overcoming the Barriers

1. Failure to meet all of the Unique Patient Identifier's operational characteristics

2. Failure to meet all of the Unique Patient Identifier's component requirements

3. Inability to fulfill all of the basic functions of a Unique Patient Identifier

4. Development of the necessary communication technology and computer software to facilitate the exchange of information from multiple institutions with multiple identifiers for the same patient

5. Timeliness.

IX. Solutions to the Barriers:

The Directory Service is not a Unique Patient Identifier Proposal. It must include a Unique Patient Identifier solution in addition to its cross-referencing process. The solutions to barriers includes:

1. Inclusion of the missing Unique Patient Identifier's operational characteristics

2. Inclusion of the missing Unique Patient Identifier's components

3. Inclusion of the missing Unique Patient Identifier's basic functions requirements

4) Development of the Directory Service software, implementation of standards, technology, communication protocols, etc.

Part Eight: Central Trusted Authority Options

An administrative infrastructure is required to manage and control the various functions relating to the issue, use and maintenance of the identifier. The lack of a mechanism to track the previous sites of care for an individual, leave a significant gap in the process of identification of a patient and his or her information from previous treatments. A Central Trusted Authority with appropriate power can help fulfill these requirements. In addition, the integrity of the patient identifier is essential to access the patient information reliably; the identifier and the demographic identification information are both highly confidential. The Central Trusted Authority can address these critical functions effectively. It can be a government agency, a semi-government entity, or a private organization. The final UPI choice will determine the choice of the Central Trusted Authority. Examples of the available options are Social Security Administration and United States Postal Service.

Social Security Administration (SSA)

The Social Security Administration has the most experience in managing a nationwide identification system.

United States Postal Service (USPS)

The Public Law 91-375, Postal Recognition Act mandates the USPS with a statutory responsibility to bind the nation together through the personal, educational, literary and business correspondence. Charles R. Chamberlain from USPS discussed with the author, the unique capability of the USPS to function as a stable, neutral and trusted third party and manage patient identification functions. USPS has a legal and constitutional infrastructure and universal presence.

United States Vital Health Records Trust

Edward Hernandez, the proponent of the LHSTR Number, recommends the creation of a national level organization. He suggests that the current Association for Vital Health Statistics, that exists in the 50 states, may be organized into a United States Vital Health Records Trust to function as a Central Trusted Authority.

Part Nine: Result of the Analysis

The outcome of this analysis is summarized in five (5) parts:

1) General Findings relating to Unique Patient Identifier requirements, functions, characteristics, components and capabilities

2) Compliance with Unique Patient Identifier Requirements including ASTM Conceptual Characteristics, Operational Characteristics and Components Requirements and Basic Functions

3) Compliance Summary

4) Compliance Matrix for ASTM Conceptual Characteristics

5) Compliance Matrix for Operational Characteristics, Components Requirements Basic Functions.

1) General Findings

GF1. Patient Identifier is an integral part of patient care

Positive identification of the patient is required for the delivery of care. Healthcare organizations perform this function with the use of a Patient Identifier. Reliable Patient Identifiers are mandatory for sensitive procedures, such as blood transfusion, invasive testing, surgical procedures and medication administration. They are routinely used for 1) ordering and reporting the results of tests, procedures and medications, 2) coordinating the multi-disciplinary patient care delivery processes and 3) managing all administrative functions, such as scheduling, billing and coordination of benefit. Therefore, Patient Identifiers are an integral part of the process of delivery of care.

GF2. Patient Identifier is an Integral Part of Patient Information

A Patient Identifier accurately and uniquely identifies the patient and his/her medical information. Clinical documentation including results, observations, diagnosis, procedures, medication, progress, outcomes, etc. is based on the Patient Identifier. It is vital for the management of automated information and manual medical record functions including compilation, filing, storage, retrieval and communication. Patient Identifier is mandated by regulatory authorities as a component of the medical record. Therefore, it is an integral part of the patient care information.

GF3. The Need for a Unique Patient Identifier is Urgent and Essential

The industry is currently using patient identifiers for day to day patient care functions. The continuum of care across multiple providers, access to information from multiple care settings that are necessary during the delivery of care and the retrieval and assembly of relevant patient care information from past episodes of care across different times require the use of a Unique Patient Identifier. Unique Patient

Identifiers are required to facilitate the aggregation of population-based health information for research and development purposes. The identifiers used currently are not unique across the national healthcare system. Therefore, they present problems in 1) accessing or integrating information from different providers and their computer systems, 2) aggregating and providing a lifelong view of a patient's information and 3) supporting population-based research and development. Making the Patient Identifier unique across the nation brings significant improvements to the entire industry. The need for a Unique Patient Identifier is vital and therefore, not a debatable issue.

GF4. Industry pursues an aggressive solution for a Unique Patient Identifier

Recent advancements in computer and communication technologies have opened up new opportunities for interoperability among geographically distributed healthcare organizations. These new opportunities have the potential to facilitate the integration of patient care information from multiple providers and different times to form a lifelong record of a patient. They can provide communication capabilities to enable online and realtime consultations, coordination of care, telemedicine/remote care, etc. Unique Patient Identifier plays an indispensable role as the interoperability key in turning these possibilities into reality. The response from the industry to meet this important need is impressive. It has come up with a total of 12 new proposals for the Unique Patient Identifier. The proponents include provider organizations, healthcare professionals from different disciplines, software developers, standards developing organizations, information technology professionals, industry consortium and professional organizations.

GF5. The Privacy, Confidentiality & Security of Patient Information Do Not Preclude the Use of Unique Patient Identifier

The privacy and confidentiality of patient care information is a difficult challenge facing the entire healthcare industry and cannot be ignored. In order to fully and effectively address the privacy requirements, the following additional steps must be taken at national, organizational and individual levels:

1. Federal Privacy, Confidentiality and Security Legislation relating to healthcare information including the use of Patient Identifiers (national level)

2. Appropriate organizational policies and procedures to protect patient care information maintained by organizations (organizational level)

3. Appropriate access control to prevent unauthorized access including software access security, physical access security, encryption protection such as encrypting the identifier itself and authentication mechanism to ensure legitimate access (organizational level)

4. Audit trails for tracking inappropriate access and preventive steps against possible misuse (organizational level)

5. The above protective measures must be evaluated on an ongoing basis and

improved continuously (organizational level)

6. Public education on the importance of privacy & confidentiality and user training to enforce patient's privacy and confidentiality (individual level).

The critical need of the industry such as the Unique Patient Identifier cannot be sacrificed due to the failure to adequately address the necessary privacy safeguard and subject the patient care to unnecessary risks. A Unique Patient Identifier is an integral part of the patient care information. Therefore, it requires the same confidentiality and security protection as the patient care information itself. The privacy, confidentiality and security requirements do not preclude the use of a Unique Patient Identifier. In fact, the Unique Patient Identifier can help meet these requirements by standardizing and strengthening access control and eliminating the repeated use of personal identification information.

GF6. A Judicious Design of the Unique Patient Identifier Can Fulfill the Patient Care Need and Protect the Privacy and Confidentiality of Patient Information.

Unique Patient Identifier requires a design architecture that will keep the identification of patient care information and its access as two distinct and separate functions within healthcare. The identifier's role is limited merely to identify the patient record by accessing only the identification segment of patient record and not its content. Access control deals with the authentication of the user (e.g. validation of user ID and password), verification of access privileges, audit trails, physical security, etc. This will enable the identification function and security access to complement and support each other by performing exclusively their own distinct roles rather than assuming each other's. This architecture consists of the following design approaches:

1. Separate identification from access
2. Limit the Identifier's capability and use it for identification alone (not to provide access to the content of the patient information)
3. Design the Identifier to be unique
4. Utilize a standard/uniform set of identification information
5. Design Access Control to include
    a) authentication
    b) access privilege
    c) audit trails
    d) separate access to ID segment and patient care information
6. Provide the option to store Unique Patient Identifier in an encrypted format
7. Support the option to communicate it in an encrypted format.

GF7. Effective Ongoing Organizational Measures are required to Support Patient Identification and Confidentiality

The judicious design discussed above must be supplemented by appropriate ongoing organizational measures to protect the patient care information. A failsafe access

control mechanism including software security, physical access security, encryption protection and an authentication mechanism must be in place to prevent unauthorized access and ensure legitimate access. The security measures include audit trails for tracking inappropriate access and preventive steps against possible misuse. They must be evaluated on an ongoing basis and improved continuously.

GF8 Uniform Federal/State Legislation is Required to Protect the Privacy and Confidentiality of Healthcare Information

In order to ensure the privacy and confidentiality of patient care information beyond organizational boundaries, uniform federal and state privacy and confidentiality legislation is required. Such legislation must protect the Unique Patient Identifier from misuse, prevent unauthorized access to patient care information, illegal linkages and discrimination based on patient care information.

GF9. Individual Responsibility Must be Instilled Through Education

Protection of patient care information is also the responsibility of individuals that handle them. Therefore, individual responsibility for the privacy and confidentiality of patient information must be instilled through staff and user training, education and reinforcement among the users and consumers. Public education of the value of privacy and confidentiality of healthcare information and the legal consequences of violation must be provided nation-wide.

GF10. Unique Patient Identifier Requires an Issuing Authority

The issue and maintenance of the Unique Patient Identifier, the identification information and their use need to be handled either under a centralized or decentralized administration. The ASTM Standards Guide requires a Central Trusted Authority for this purpose. Example of available options are Social Security Administration and the United States Postal Service. The LHSTR Number proposal recommends the creation of a United States Vital Health Records Trust for this purpose.

GF11. Unique Patient Identifier Prevents Exposure and Protects Patient's Privacy

A Unique Patient Identifier eliminates repetitive use and disclosure of an individual's personal identification information (i.e. name, age, sex, race, marital status, place of residence, etc.) for routine internal and external communications (e.g. orders, results, medication, consultation, etc.) and protects the privacy of the individual. It helps preserve the patient anonymity while facilitating communication and information sharing.

GF12. Unique Patient Identifiers Help Standardize the Method of Accessing Patient Care Information

The use of a Unique Patient Identifier to access patient care information helps standardize the access method and enables organizations to use a single point of access. The direct use of the patient demographic information for the purpose of identification will increase the level of exposure and subject the patient to unnecessary privacy risks. The use of non-standard access methods instead of the

Unique Patient Identifier method will be difficult to control and monitor. Therefore, it will increase the potential for the violation of privacy and confidentiality of patient information.

GF13. Unique Patient Identifier Strengthens Access Control to Protect the Privacy, Confidentiality and Security of Health Information

The single point of access and the standard access method enable organizations to plan and implement the necessary access control. They can monitor the access and continuously improve and strengthen the access control with appropriate measures. A valid Unique Patient Identifier provides both the necessary focused control as well as timely and reliable access. Accessing through a single Unique Patient Identifier also:

I. facilitates focusing on a single access point for the purposes of verifying access privileges, tracking violators, keeping audit trails and preventing unauthorized access.

ii. facilitates an individual's identification information and health information to be kept separate to ensure accurate identification of the individual without allowing access to the individual's health information.

iii. permits use of additional authentication elements such as a valid user ID, pass word, etc. to verify access privileges.

iv. enables industry to establish and follow a nation-wide standards for identification and access that can both detect the violations and facilitate preventive measures.

v. helps maintain appropriate access security for both the identification information and health information of individuals.

GF14. Multiple Identifiers Inhibit Timely Access

Use of multiple identifiers for the same patient keeps the information fragmented and isolated and makes it difficult for timely access for care by providers from other locations. It may make the unauthorized linkage difficult, but by the same token, it also hurts legitimate purposes such as timely access to information and delivery of care.

GF15. Access Security Controls the Privacy and Confidentiality, and not the Identifier

Unique Patient Identifier must accurately identify the patient information. However, access to such information must be controlled with appropriate access security including, physical security, system controls, user ID, password authentication, audit trails, etc. The role of the access security is to grant access for authorized use and prevent unauthorized use. The role of a Unique Patient Identifier is to assist the authorized use by accurately identifying the patient and his/her information.

GF16. Unique Patient Identifier is Made up of Six (6) Critical Components

Unique Patient Identifier is made up of six (6) components essential for its

performance. They are:

1. Identifier (numeric, alphanumeric, etc.) Scheme
2. Identifying Information
3. Index
4. Mechanism to hide or the tool to encrypt the Identifier
5. Technology infrastructure including the software, hardware and communication technologies to search, identify, match, encrypt, etc.
6. Administrative infrastructure including the Central Governing Authority.

These components must work together to effectively fulfill the objectives of the Unique Patient Identifier.

GF17. Identifier Components and Operational Characteristics are Critical to the Basic Functions of Unique Patient Identifier

The focus, on the choice of a Unique Patient Identifier, its content/format and assignment, alone will not address the patient identification need. It can neither protect the privacy and confidentiality of patient care information nor assure its accurate identification. These functions depend also on the maintenance of current identification information, security measures such as access security and secure communication, and appropriate technology infrastructure. The six (6) identifier components and operational characteristics provide these capabilities, and in essence give the identifier the necessary functionality.

GF18. Reliable Identification and Confidentiality Require Provider/User Organizations' Participation and Compliance

Although most of the ASTM characteristics such as *assignable, accessible, identifiable,* etc. deal with compliance by the Issuing Authority, healthcare information is created, maintained, accessed and used at healthcare organizations. Positive identification of individuals and access to their patient care information are required at these sites. Therefore, the major threat to the privacy of patient care information occurs at the user end where the information resides rather than at the issuing end. Appropriate control and security are therefore, required both at the point of issue of Unique Patient Identifier such as a Central Trusted Authority and the point of use, such as a provider organization. In order to assure reliable and accurate identification, the identification information must be accurate and current both at the point of issue of the identifier and the provider organizations. Compliance with ASTM conceptual characteristics by the Issuing Authority is necessary for a prompt, reliable and accurate issue of identifiers.

GF19. Check-digits and Encryption are Common to All Options

Check-digit protects against transcription errors and assures accuracy. It can be used to support any numeric identifier. Encryption ensures storage and communication in a secure format. All the Unique Patient Identifier options discussed in this report can make use of this feature. Different encryption schemes yield different encrypted identifier for the same patient. Only authorized users can decrypt

the encrypted identifier. Encryption may be used when protection is needed or on a permanent basis. It may be administered either by a Cental Trusted Authority or by provider organizations themselves.

GF20. Development of Technology Infrastructure Requires Direction, Support and Coordination

Alternatives to the Unique Patient Identifier options CORBAMed, HL7 and Directory Service address a critical but only one of the identifier components, namely, the technology infrastructure/software solution. Although these are not identifier initiatives, the selection and industry-wide adoption of a Unique Patient Identifier will help their development and strengthen their capabilities. Basic functions of the Unique Patient Identifier depend on the technology infrastructure.

GF21. Critical Functions are Independent of Identifier Scheme/Value of the Identifier

Critical functions such as access control, identification information, administrative and technology infrastructure, etc. are independent of the numbering scheme or the value of the identifier (i.e. the actual choice of the Unique Patient Identifier). They are not unique or proprietary to any particular Unique Patient Identifier (numbering) scheme or value. They can be implemented with any one of the five Unique Patient Identifier options.

2) Compliance with Unique Patient Identifier Requirements

i. Compliance with ASTM Conceptual Characteristics

a) Unique Patient Identifiers:

All Unique Patient Identifier options meet almost all of these criteria. None of these options are "based on existing standards". Sufficient information is not available to compare their "cost effectiveness". Although the ASTM Standard Guide requires the Unique Patient Identifier to be "public", it is an integral part of the patient's health information and requires the same protection as the patient care information. All six options are in general compliance with the remaining ASTM characteristics.

1. Enhanced SSN complies fully with 27 criteria and partially with 1.

2. Sample UHID complies fully with 25 criteria and partially with 1.

3. Unique Patient Identifier based on the Bank Card Method complies fully with 27 criteria.

4. The Personal Immutable Characteristics based Model UPI complies fully with 23 criteria and partially with 1.

5. The LHSTR Number complies fully with 24 criteria and partially with 2.

6. The Unique Patient Identifier based on Biometrics complies fully with 20 criteria and partially with 3.

b) Non-Unique Patient Identifiers:

The Medical Record Number and Medical Record Number with a Provider Prefix do not meet several of the ASTM criteria such as *unique, secure, disidentifiable, mappable, controllable, longevity, retroactive, centrally governed and universal.* The Cryptography-based Identifier is not unique and not suitable for manual use. According to its proponents it cannot be used as a patient identifier until the use of computerization is universal throughout the healthcare organizations. In general, Non Unique Patient Identifiers do not meet the ASTM criteria adequately.

c) Alternatives to Unique Patient Identifier

Of the five (5) alternatives to the Unique Patient Identifier, Manual Process was not evaluated and the remaining four were analyzed. CORBAMed PIDS, HL7 Mediation and Directory Service are not identifiers. Therefore, they do not meet any of the ASTM criteria except "networked". FHOP's Standard Data Set does not meet 21 of the 30 criteria. It meets only *identifiable, mergeable, linkable, mappable, focused, deployable, unique, networked and incremental* criteria.

ii. Compliance with Operational Characteristics

Enhanced SSN is the only option that meets almost all of the Operational Characteristics. Only the proposed enhancements are not operational. Except for the Social Security Number, none of the six (6) Unique Patient Identifier options or the three (3) Non Unique Patient Identifiers or the five (5) alternatives are currently used as a Unique Patient Identifier. SSN is used across the nation by VA hospitals, Medicare and the Department of Defense. Most of the new proposals are at a conceptual level and not ready for implementation. A modified UHID is being tested by three VA hospital locations in Florida as an Internal Control Number (ICN). FHOP has tested the Common Core Data Elements on three databases of varying sizes. The Directory Service is being used on a limited scale for mental health projects in the state of Georgia. CORBAMed is in the RFP process and HL7 in the planning phase.

For CORBAMed PIDS, HL7 Mediation, Cryptography-based Identifier and FHOP's Standard Data Set, the software technology needs to be developed. They are, therefore, not ready for implementation. None of the options, except SSN, has the necessary administrative and technology infrastructure in place and their timely implementation is questionable. The LHSTR Number option does not require patient participation and uses birth certificate information for its issue. This may enable faster implementation.

iii. Compliance with Components Requirements

Enhanced SSN is the only option that meets all of the components requirements. Other options address only the identifier (format) component and its characteristics,

and not the remaining five components. While all the options recognize the role and importance of the six components of Unique Patient Identifier, none provides a solution consisting of all the six components. The Sample UHID's scope does not include implementation issues. Although it indicates the need for these five components, it does not address them in detail. The LHSTR Number option includes a three (3) level patient identification information and the 3rd level tracks the previous episodes of care. Encryption is included in Enhanced SSN, Sample UHID, LHSTR Number and Cryptography based ID. CORBAMed PIDS, HL7 Mediation and Directory Service focus on software and communication (technology) infrastructure. SSA has existing administrative and technology infrastructures. LHSTR Number proposal recognizes the need for an administrative infrastructure and suggests an organization such as SSA.

iv. Compliance with Basic Functions Criteria

a) Identification of Individuals for Delivery of Care and Administrative Functions

These activities take place during the course of active delivery of care. Care providers and administrative staff use the identifiers to interact with the patient and among themselves. Only those identifiers that are concise and manageable in size fully meet these requirements and support identification functions and communication during delivery of care. Identifiers, that are not concise are not suitable for manual use and verification in oral and written communications, consultations and interaction among care providers and care team members. The Enhanced SSN, existing Medical Record Number and Medical Record Number with Provider Prefix appear to be more suitable for these functions than lengthy identifiers such as Sample UHID, LHSTR Number, Cryptography-based Identifiers. Alternatives such as CORBAMed PIDS, HL7 Mediation and Directory Service do not meet this criteria.

b) Identification of Information

Identification of information is required for a) coordination of multi-disciplinary care process, b) medical record keeping/organization of patient information, c) lifelong health record and d) aggregation of health information. Options other than the Enhanced SSN and the Medical Record Number are only at a conceptual level. Most of them do not comply with all of the Unique Patient Identifier component requirements and operational characteristics. Some options have their concepts well developed and some are at a preliminary level. Options such as Bank Card Method, Cryptography-based identifiers, etc. need a significant amount of additional development to compare their capabilities. Their ability to support these basic functions is unknown. The Sample UHID, the LHSTR Number and Unique Patient Identifier based on Personal Immutable Properties are examples of well developed concepts. However, to support these basic functions, they must have the remaining Unique Patient Identifier Components and the required operational characteristics in place. The analysis indicates their potential for identifying information once the rest of the Unique Patient Identifier Components and Operational Characteristics are in place. The Enhanced SSN meets these basic functions criteria and SSN is currently used for these purposes. CORBAMed PIDS, HL7 Mediation and Directory Service help linkage and aggregation of health information via software searching and matching. But they do not directly support record keeping or information

management. They are not identifiers but software tools for searching and matching information. The FHOP option uses its data set (containing personal identification information) every time to perform the basic functions.

c) Privacy, Confidentiality & Security

Access Security: Only Enhanced SSN addresses the access security of health information via the use of a Unique Patient Identifier. CPRI recommends organizational security measures and federal legislation for this purpose. Other options do not address this important function.

Format & Content: Although the SSN format includes the time and place of its issue, for healthcare purposes it is considered as non-identifiable and content-free. The Sample UHID, LHSTR Number and Medical Record Number are content-free. Once again CORBAMed PIDS, HL7 Mediation, Directory Service are not identifiers, but they contain the patient's personal identification information and use them for searching, matching and verification.

Encryption: Enhanced SSN, Sample UHID, LHSTR Number and Cryptography based Identifier use encryption to disidentify individuals.

d) Improve Health/Reduce Cost

SSN is currently in use and SSA provides the necessary administrative and technology infrastructure throughout the nation. The SSA is continuing to evaluate options to improve its identification system including the card and the procedure. Therefore, Enhanced SSN can be implemented in the least amount of time and expenditure. Other options such as Sample UHID require development of the remaining Unique Patient Identifier Components, technology and administrative infrastructure, implementation plan, etc. Therefore, it involves additional resources and time. The LHSTR Number option uses the existing birth certificate information to speed up the assignment of identifiers. The options at levels where their concepts are not fully developed requires the greatest amount of time and resources to implement.

3) Compliance Summary

CS1. All of the Unique Patient Identifier options (SSN, ASTM Sample UHID, LHSTR Number, Personal Immutable Characteristics based Identifier, Bank Card Method and Biometrics) are in general compliance with the ASTM Conceptual Characteristics with the exception of Biometric method which does not meet 7 of the 30 characteristics.

CS2. Non-Unique Patient Identifier options (Medical Record Number, Medical Record Number with Provider Prefix and Cryptography based Identifier) do not meet the ASTM conceptual characteristics adequately.

CS3. Alternatives to Unique Patient Identifier (CORBAMed, HL7, Directory Service, FHOP Standard Data Set and Manual Process) are significantly non- compliant with

the ASTM conceptual characteristics.

CS4. Those options that did not comply with the conceptual characteristics also did not comply with the rest of the requirements including Operational Characteristics, Unique Patient Identifier Component Requirements and Basic Function Requirements.

CS5. Of the five Unique Patient Identifier options that fared well at the conceptual level, Enhanced SSN is the only option that complied with the operational characteristics and component requirements. The remaining four are not operational and they still remain as concepts. They also did not meet the ASTM criteria *concise* and *usable*.

CS6. Of these remaining four, the Sample UHID is a well developed concept followed by the LHSTR Number and Personal Immutable Character-based Identifier. Even as a concept the Bank Card Method requires a significant amount of additional development.

CS7. SSN is used by 20% of the public as a Unique Patient Identifier and the SSA is evaluating different options to enhance SSN and fix its current problems.

CS8. A modified Sample UHID is piloted by the Florida VISN as an internal control number. However, it is used in conjunction with SSN. SSN continues to be the patient identifier (embossed, bar coded and included in the magnetic stripe of their ID card) because the ICN is too long for veterans to remember and users to handle.

CS9. The MRI's proposal, Medical Record Number with Provider Prefix, directs the focus away from patient identification to information identification. It designates the Primary Care Physician as the curator to track the previous sites of care for an individual. Therefore, it seems to neglect some of the basic functions of the Unique Patient Identifier.

CS10. Alternatives to Unique Patient Identifier address only one of the components of the Unique Patient Identifier (e.g. technology infrastructure and identification information) CORBAMed, HL7 and Directory Service address the technology infrastructure/software solution and the FHOP option addresses data standardization.

CS11. Options indicate preference for organizations similar to Social Security Administration (SSA) and United States Postal Service (USPS) to address the Administrative Infrastructure component and serve as the Central Trusted Authority. However, the organizational structure, authority, policies and procedures need to be defined and the Infrastructure established. SSA appears to have the most of the processes currently in use.

4) Compliance Matrix for ASTM Conceptual Characteristics

COMPLIANCE WITH ASTM CONCEPTUAL CHARACTERISTICS													
Requirements	**SSN**	**UHID**	**BCM**	**CRYP**	**IMM**	**BIO**	**LHST**	**MRN**	**MRPR**	**CORB**	**FHOP**	**HL7**	**DIR**
FUNCTIONAL:													
Accessible	Y	Y	Y	Y	Y	P	Y	Y	Y				
Assignable	Y	Y	Y	Y	Y	P	Y	Y	Y				
Identifiable	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		
Verifiable	Y	Y	Y	Y	Y	N	Y	Y	Y				
Mergeable	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		
Splittable	Y	Y	Y	Y	Y	Y	Y	Y	Y				
LIFELONG HEALTH RECORD:													
Linkable	Y	Y	Y	Y	Y	Y	Y	P	Y	Y	Y	Y	Y
Mappable	Y	Y	Y	Y	Y	Y	Y		Y		Y		
CONFIDENTIALITY:													
Content-free	Y	Y	Y	N	N	N	Y	Y	N	N	N	N	N
Controllable	Y	Y	Y	Y	Y	Y	Y						
Healthcare Focused	P	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
Secure	Y	Y	Y	Y	Y	Y	Y						
Disidentifiable	Y	Y	Y	Y	Y	Y	Y						
Public	N	N	N	N	N	N	N	N	N	N	N	N	N
STANDARDS:													
Based on Industry Standards	N	N	N	N	N	N	N	N	N		N		
Deployable	Y	Y	Y	Y	Y	Y	Y	Y	Y		P		
Usable	Y	P	Y	P	P	P	P	Y	Y		P		
DESIGN:													
Unique	Y	Y	Y	N	Y	Y	Y	N	N		Y		

COMPLIANCE WITH ASTM CONCEPTUAL CHARACTERISTICS													
Requirements	SSN	UHID	BCM	CRYP	IMM	BIO	LHST	MRN	MRPR	CORB	FHOP	HL7	DIR
Repository-based	Y	Y	Y	Y	Y	Y	Y	Y	Y		N		
Atomic	Y	Y	Y	Y	N	Y	Y	Y	Y		N		
Concise	Y	N	Y	N	N	N	N	Y	Y		N		
Unambiguous	Y	Y	Y	N	Y	Y	P	P	P				
Permanent	Y	Y	Y	Y	Y	Y	Y	Y	Y		P		
Centrally Governed	Y	Y	Y	Y	Y	Y	Y	N	N		N		
Networked	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
Longevity	Y	Y	Y	Y	Y	Y	Y						
Retroactive	Y	Y	Y	Y	Y	Y	Y						
Universal	Y	Y	Y	Y	Y	Y	Y						
Incremental	Y	Y	Y	Y	Y	Y	Y		Y		Y		
ENHANCED HEALTH STATUS:													
Cost-effectiveness	Y	U	U	U	U	N	U	N	U	U	U	U	U

Legend:

Y	Yes
N	No
P	Partial
U	Unknown
Blank Cell	Not Applicable

5) Compliance Matrix for Operational, Components and Basic Functions Requirements

COMPLIANCE WITH OPERATIONAL, COMPONENT & FUNCTIONAL REQUIREMENTS													
Requirements	**SSN**	**UHID**	**BCM**	**CRYP**	**IMM**	**BIO**	**LHST**	**MRN**	**MRPR**	**CORB**	**FHOP**	**HL7**	**DIR**
OPERATIONAL:													
Operational as UPI	Y	N	N	N	N	N	N	N	N	N	N	N	N
Existing Infrastructure	Y	N	N	N	N	N	N	N	N	N	N	N	N
Readiness of Technology	Y	Y	Y	N	Y	Y	Y	P	P	Y	Y	Y	Y
Timely Implementation	Y	U	N	N	U	N	U	N	U	N	N	N	N
Identification Information	Y	U	U	U	U	U	Y	P	Y	N	P	N	N
COMPONENT:													
Identifier	Y	Y	P	N	Y	P	Y	N	N	N	N	N	N
Identification Information	Y	U	U	U	U	U	Y	N	P	N	P	N	N
Index	Y	U	N	N	U	N	Y	N	P	N	N	N	N
Protect/Mask	Y	Y	N	Y	N	N	Y	N	N	N	N	N	N
Technical Infrastructure	Y	N	N	N	N	N	N	N	P	N	N	N	N
Admin. Infrastructure	Y	N	N	N	P	N	P	N	P	N	N	N	N
BASIC FUNCTIONS:													
Identification of Individual:													
Delivery of Care	Y	P*	U	N	P*	U	P*	N	N	N	N	N	N
Admin. Functions	Y	P*	U	N	P*	U	P*	N	N	N	N	N	N
Identification of Info:													
Multi-discipl. Care	Y	P*	U	N	P*	U	P*	N	N	N	N	N	N
Medical Rec. Keeping	Y	P*	U	N	P*	U	P*	N	N	N	N	N	N

COMPLIANCE WITH OPERATIONAL, COMPONENT & FUNCTIONAL REQUIREMENTS													
Requirements	**SSN**	**UHID**	**BCM**	**CRYP**	**IMM**	**BIO**	**LHST**	**MRN**	**MRPR**	**CORB**	**FHOP**	**HL7**	**DIR**
Lifelong Health Record	Y	P*	U	P	P*	U	P*	N	N	P	N	P	P
Aggregation of Info	Y	P*	U	U	P*	U	P*	N	N	P	N	P	P
PRIVACY & SECURITY:													
Access Security	Y	U	U	U	U	U	U	N	N	U	U	U	U
Content-free	Y	Y	Y	N	N	N	Y	Y	N	N	N	N	N
Protect/Mask	Y	Y	N	Y	N	N	Y	N	N	N	N	N	N
IMPROVE STATUS:													
Cost-effectiveness	Y	U	U	U	U	U	U	N	U	U	U	U	U

Legend:

Y Yes

N No

P Partial

P* Partial Contingent upon compliance with Component Requirements and Operational Characteristics

U Unknown

Part Ten: Available Courses of Action

The result of the analysis indicates that none of the options in its present form is a perfect choice. Existing options require enhancements to add features/functions and correct existing problems. New options are at a conceptual level and lack operational characteristics and several of the required components. But, they also embody new ideas and features. Each one of them brings its own unique strength. Collectively, they account for the various requirements of the Unique Patient Identifier. However, none of the options by itself meets all of the requirements. Some of the identifier concepts are not fully developed. Unique Patient Identifier is a critical need of the healthcare industry with impact on the privacy of individuals. The nation must adopt a method that can fully address the people's need including protection of their privacy, and it cannot limit its choice to incomplete ideas and methods.

An Ideal Unique Patient Identifier

This study analyzed both the Unique Patient Identifier requirements (including conceptual, operational, functional and components requirements) and the various available options (13 altogether including MRN). The analysis and examination of the Unique Patient Identifier requirements highlight the importance of all of the components that make up the identifier, their operational characteristics and functional capabilities. These components include:

1. An Identifier (numeric, alphanumeric, etc.) Scheme

2. Identification Information

3. Index

4. Mechanism to hide or the tool to encrypt the Identifier

5. Technology infrastructure to search, identify, match, encrypt, etc.

6. Administrative infrastructure including the Central Governing Authority.

Use of Unique Patient Identifier and maintenance of up-to-date identification information, security and access control require multiple participants including the patient, issuing authority, system developers, provider organizations and other users to cooperate and support the identifier functions. These Unique Patient Identifier components facilitate their participation.

Analysis of the various available options reveals that they focus more on the Identifier Scheme component and less on the remaining five components. The ASTM Guide treats implementation and policy issues to be beyond its scope. Results from ASTM's own evaluation of its Sample UHID indicate that several important characteristics such as *Accessible, Assignable, Controllable, Governed, Identifiable, Secure* and *Unique* depend on implementation and policy issues that are beyond the

scope of its Guide. As a result, all of the Unique Patient Identifier options meet the ASTM conceptual characteristics almost equally with minor exceptions, but leave a wide gap in addressing the components that are necessary to support all of the functions of the Unique Patient Identifier and its operational requirements. Consequently, SSN, currently operational as a Unique Patient Identifier, emerges as the only option that meets both the operational characteristics and component requirements of a Unique Patient Identifier.

A careful overall analysis reveals that in fact, it is the remaining components, such as Administrative and Technology Infrastructures, Identification Information (demographic information) and Security Encryption, that give functionality to the identifier components. They address specifically:

1. the Administrative Infrastructure to issue and maintain UPIs

2. the maintenance of accurate and up-to-date identification information of individuals by both the issuing entity and the provider/user organizations

3. secure communication including the use of encryption to protect the identifier

4. software solutions and error checking mechanism including the use of check-digits to prevent transcription errors, etc.

5. access control security to protect privacy of individuals, etc.

These critical functions are independent of the numbering scheme or the value of the identifier (i.e. the actual choice of the Unique Patient Identifier). They are not unique or proprietary to any particular Unique Patient Identifier (numbering) scheme or value. They can be implemented with any one of the five Unique Patient Identifier options.

This, in fact, enables us to separate the identification scheme from all other components. Since key functions such as access control, maintenance of up-to-date identification information and secure communication are addressed by the other components, a simple user friendly Unique Patient Identifier that is suitable for use by both humans and computers constitutes an ideal choice for the Unique Patient Identifier. We can, therefore, now choose a simple and reliable identification scheme and equip it with all of the required functionality by adding the remaining five components.

Available Courses of Action

In order to fulfill the current Unique Patient Identifier need of healthcare industry, the following three (3) courses of action are available:

I. Enhance an existing option

II. Develop a conceptual level option to fruition

III. Develop or facilitate the development of an ideal option.

I. Enhance an existing option

The only option that is being currently used as a Unique Patient Identifier is SSN. It is used by 20% of the population as a Unique Patient Identifier. It is also collected, stored and used as part of patients' demographic information by most of the healthcare organizations. SSN is also used as a secondary and confirmatory identifier by a large number of provider organizations. With its existing administrative and technology infrastructures, and operating procedures, SSN is at a higher level of readiness for implementation than other options. It meets the conceptual and operational characteristics, and component and basic functions requirements. Only the proposed enhancements need to be implemented. It is likely to require relatively less time, effort and resources because of its current use and readiness. According to a 1993 Harris poll (Health Information Privacy Survey 1993), the majority of the American population and organizational leaders favor SSN as a patient identifier. It offers an early solution while allowing other options that are not fully developed to mature.

Use of SSN by other industries presents the potential for linking an individual's health information with his or her financial or social information, resulting in discrimination and financial harm. However, a close look at these risks reveals that in fact, the security risk related to SSN is common to all Unique Patient Identifier options. In the absence of the necessary access control, linkages are possible under any of the options. It is easy for a computer to map data based not only on SSN, but any one, or more identification data elements such as name, address, sex, age, etc. and create linkages and references regardless of the identifier. Other industries have these identification data elements on individuals as well. It is the access control that protects against unauthorized access. The identifier design that separates the identification from access is the key to securing healthcare information. Without this design, both SSN and a brand new identifier will have a significant amount of exposure. As discussed in the Judicious Design section earlier, the Unique Patient Identifier's design should support its storage and transmission in an encrypted format to protect the identity of the individual.

The Enhanced SSN includes the use of encryption to mask the SSN. Depending on the need, it can be used in the encrypted format all the time or only when protection is needed. The encryption scheme can be administered either by a Cental Trusted Authority or by provider organizations themselves. Therefore, with the appropriate access control discussed earlier, the Enhanced SSN can be used as a valid Unique Patient Identifier.

The existing error level in SSN presents a threat to its accuracy and integrity. The Enhanced SSN proposal includes enhancements such as check-digits to address SSN's current problems and improve its capabilities further. The SSA is currently evaluating multiple options to enhance the SSN to eliminate errors and improve its security, integrity and related processes. It has submitted a report to the Congress outlining

such options. In fact, the features and functions that are included in the new options can also be added to SSN. Other enhancements in the Enhanced SSN option include ID for emergency use, ID for individuals ineligible for SSN, increased SSN capacity, etc.

SSN is a simple, user friendly Unique Patient Identifier that can be used by both computers and healthcare professionals. Since it is already in use at most of the provider organizations, it is relatively easy to expand its role as the Unique Patient Identifier.

II. Develop from a conceptual level method

The remaining options discussed in this report, with the exception of Medical Record Number, are at a conceptual level. (A modified Sample UHID is piloted as an Internal Control Number to create an MPI, and the FHOP Standard Data Set is being tested on patient care data bases to eliminate duplicate records). These options mainly address the identifier scheme and lack remaining components and operational characteristics. They require significant development, including the following:

1. the required Unique Patient Identifier components
2. the administrative infrastructure
3. the required technology infrastructure
4. an implementation plan
5. effective operating procedures and policies.

Some of the options provide identifiers that are too long for manual computation and use. Such lengthy identifier are difficult for the patient to remember and provider organizations to handle. Therefore, the impact on the operation of the provider organizations and users must be fully analyzed. These options also need the same level of Organizational Access Security and Design features and federal privacy legislation.

A well developed concept, such as Sample UHID or LHSTR Number or one of the other options, may be chosen based on their ability to meet the ASTM Conceptual Characteristics. It can be developed further to include those characteristics and components that are missing. Implementation of a new choice will avoid any carry over problems and provide a fresh start. But it will require a relatively longer time frame to develop, test and deploy than enhancing and adopting an existing option. Therefore, the impact of time, resource, effort and cost effectiveness must be thoroughly analyzed. Because of the developmental status of these options, it is possible that this choice may prove to be the most expensive and time-consuming.

III. Facilitate the development of an ideal solution that includes all of the requirements

None of the proposals including the ASTM Sample UHID, meets all thirty (30) ASTM conceptual characteristics. Most of them are not concise and not suitable for manual calculation and use. Some are not content-free. All are at a conceptual level,

some with their concept not fully developed. Each option has different strengths and weaknesses. But collectively they represent all of the required characteristics of an ideal Unique Patient Identifier.

1) Therefore, instead of limiting the industry to one of these options, an ideal Unique Patient Identifier can be developed by consolidating all of the required characteristics. The time frame for its implementation will be comparable to that for one of the proposed conceptual level Unique Patient Identifiers. This course of action will yield the best possible Unique Patient Identifier choice.

2) Alternatively, instead of integrating together the independent proposals, we can foster the independent growth and maturity of the various options. This course of action will provide an opportunity for the competing options to mature. It can be accomplished by establishing leadership, setting the direction and functioning as a catalyst and facilitator to support and promote the growth and development of the various options. Over a period of time, the industry initiatives will mature and multiple efforts converge. Their capability and suitability can be assessed at appropriate intervals, taking into account the passage of the Privacy, Confidentiality and Security legislation by the U.S. Congress. There is an inherent risk that the progress of the options may remain stagnant. Appropriate leadership and support can bring success and benefit to this option. This course of action may cause delay and postpone the implementation of the urgently needed Unique Patient Identifier.

The Need for Leadership

The revolution currently taking place in healthcare, information and communication industries presents both challenges and opportunities for patient care, research and cost saving. Unique Patient Identifier is a vital link to achieve innovation and quality healthcare. A simple and user friendly UPI that can fulfill all the requirements including security and confidentiality is the need of the hour. The healthcare industry has put forth options and alternative (total 12).

The new options for the Unique Patient Identifier still remain as concepts. For them to progress and materialize, a strong leadership is required to take the process in the right direction. Waiting for the various options to mature and succeed by themselves may not fulfill the need adequately or in a timely manner. On the other hand, existing options, such as SSN requires implementation of several enhancements proposed. In addition, appropriate design, architecture and procedures need to be implemented in order to assure the security of the process of identification process and access control. Therefore, in both cases, a strong leadership with a clear vision is required to steer the process to a successful completion. It will help establish the necessary administrative infrastructure and define its responsibility and authority. It will facilitate the development of required technology infrastructure including development of software, communication and hardware components. Three (3) of the alternatives to Unique Patient Identifier, namely CORBAMed, HL7 Mediation and Directory Service are currently planning the development of the technology infrastructure. A strong leadership can help coordinate these processes to progress in

harmony to yield the best solution for the Unique Patient Identifier.

Part Eleven: References & Acknowledgements

References

1. Inventory of Healthcare Information Standards Pertaining to The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L. 104-191), American National Standards Institute Healthcare Informatics Standards Board (ANSI-HISB), January 1997.

2. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L. 104-191) Other Federal Legislation reviewed:

3. Medical Records Confidentiality Act of 1995 (S. 1360)

4. Fair Health Information Practice Act of 1997 (H.R. 52)

5. Medical Privacy in the Age of New Technologies Act of 1966 (H.R. 3482)

6. Health Information Modernization and Security Act (H.R. 1766/S. 872)

7. Patient and Health care Provider Protection Act of 1996 (H.R. 4315)

8. Patient and Healthcare Provider Protection Act of 1997 (H.R. 1191)

9. National Competitiveness Act of 1993 (S. 4)

10. National Information Infrastructure Act of 1993 (H.R. 1757)

11. American Standards for Testing and Materials (ASTM), Standard Guide for Properties of a Universal Healthcare Identifier (UHID), Designation: E1714-95, Approved August 15, 1995, Published October 1995.

12. ASTM E 1384-96 Guide for Content and Structure of the Computer-based Patient Record

13. ASTM E 1762-95 Guide for Electronic Authentication of Health Care Information

14. ASTM E 1769-96 Guide for Properties of Electronic Health Records and Record Systems

15. “The Debate Over a National Healthcare Identifier” - a draft article by Barry R. Hieb, M.D., Tom Payne, M.D., and Elmer Gabrieli, M.D.

16. Computer-based Patient Record Institute (CPRI), Action Plan for Implementing a Unique Health Identifier, Version 1.0. (CPRI, September 1996).

17. Computer-based Patient Record Institute (CPRI), Position Paper: Computer-Based

Patient Record Standards, April 30, 1993.

18. Computer-based Patient Record Institute (CPRI) Patient Identifier Work Group Report Version 2.1, June 1995.

19. W.L. McMullen, "Using Patient Identifiers from Legacy Systems for Healthcare Information Infrastructure", presentation at the 10th International Symposium on the Creation of Electronic Health Record Systems, Washington D.C., March 24, 1994.

20. The Department of Health and Human Services Guiding Principles for Choosing Standards For the record, 1997

21. Protecting Privacy in Computerized Medical Information, Report to the Senate Subcommittee on Federal Services, Post Office, and Civil Service, and House Subcommittee on Government Information, Justice, and Agriculture - Roger C. Herdman

22. AMIA, Position Paper on Standards for Medical Identifiers, Codes and Messages Needed to Create an Efficient Computer-Stored Medical Record, April 20, 199323. Medical Record Institute, Analysis on Patient Identifier, *Toward an Electronic Patient Record*, August 1996

24. Medical Record Institute, Position Paper 1: Patient Identifiers - Insurance Identification and Patient Identification in Healthcare, August 1993.

25. "Concept Models of Patient Identification: Issues Surrounding the Use of Social Security Numbers for Patient Identification" *Toward an Electronic Patient Record*, Medical Record Institute 1993,

26. ASC X12N TG2, Special Workgroup 8, Uniform Health Care Identification Card, Special Report, Draft 7, October 14, 1993.27. ASC X12N, Unique Identifiers for the Healthcare Industry, Technical Advisory Group White Paper, October 1993.

28. Harris-Equifax, Health Information Privacy Survey 1993 July 26 to August 26, 1993.29. Task Force on Privacy, Office of ASPE and AHCPR, Conference Proceedings, Health Records: Social Needs and Personal Privacy, February 11-12, 1993.

30. US Congress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information, May - November 1992.31. Community Medical Network Society, An Industry Perspective, A Nationwide Survey of Hospital Leadership, November 1993.

32. Gordon & Glickson P.C., Computer-Based Patient Record Survey, March 1994.

33. Institute of Medicine, Health Data in the Information Age - Use, Disclosure and

Privacy, National Academy of Press, Washington D.C., 1994

34. "Background Material on SSN and Related Discussion" offered to Staff of Heathcare Task Force April 9, 1992.

35. Willis H. Ware "Proposal for a Medical ID" offered to Staff of Heathcare Task Force April 22, 1993.

36. Paul C. Carpenter, M.D., Christopher G. Chute, M.D., Ph.D., " The Universal Patient Identifier: A Discussion and Proposal," *Proceedings of the Seventeenth Annual Symposium on Computer Applications in Medical Care, 1994,* 4 pp 49-53.

37. Lawrence O. Gostin, JD., "Privacy and Security of Personal Information in a New Health Care System," *JAMA November 24, 1993-vol270. No 20,* pp 2487-2492.

38. Lawrence O. Gostin, JD., Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization.

39. William W. Lawrence, Ph.D., "Privacy and Health Research- A Report to the U.S. Secretary of Health and Human Services," May 1997.

40. Final Report of the Task Force on the Privacy of Private Sector Health Records, Joan Turek-Brezina, September 1995.

41. "Core Health Data Elements - Report of the National Committee on Vital and Health Statistics," August 1996.

42. AHIMA Position Statement - Patient Cards, November 1993.

43. Master Patient (Person) Index (MPI)-Recommended Core Data Elements, *Journal of AHIMA* Practice Brief, July 1997.

44. ACMI Resolution February 25, 1993 on Unique Person Identification Number

45. Peter Szolovits. Ph.D., Issac Kohane, MD. Ph.D. "Against Simple Universal Health-care Identifiers," JAMIA Volume 1 Number 4 Jul/Aug, 1994, pp 316-319

46. Peter Szolovits, Ph.D., Issac Kohane, MD. Ph.D. October 4, 1994 Draft of Universal ID Proposal based on Cryptography.

47. Testimony by Denis A. Calvert, Verifone, Inc. Before Subcommittee on Domestic and International Policy of the Committee on Banking and Financial Services, United States House of Representatives, June 11, 1996

48. Using Patient Identifiers from Legacy Systems (Directory Service) by W. L.

McMullen Toward An Electronic Patient Record '97 Proceeding Manual Volume Three Healthcare Identifiers:

49. Proposal for Unique Patient Identifier, Margaret Amatyakul, CPRI.

50. Unique Patient Identifiers: An Overview, Soloman I. Appavu

51. The ASTM UHID Standard, Barry R. Hieb, M.D.

52. Patient Identifiers: Religious Dogma, Passion, and Misconceptions, Peter Waegemann

53. Potential for the Use of Social Security Number as a Healthcare Identifier. Sandy Crank, SSA

54. Master Patient Index - Presentation Material by VAH

55. UHID-based Internal Control Number - Tony Seegar, VAH, Utah.

56. Community Health Information Partnership, Master Patient Index, Request For Information (RFI), Foundatation for Health Care Quality, July 22, 1996

57. "Framework for Identifying Requirements for Standards for the National Information Infrastructure" by Information Infrastructure Planning Panel (IISP).

58. "CORBAMed Domain Task Force RFP-1, Patient Identification Services, Request For Proposal," Object Management Group, November 30, 1996

59. CORBAMed White Paper: Interface Requirements for an Enterprise Master Patient Index (EMPI), John Farmer, Care Data Systems.

60. Health Data Science Corporation's response to CORBAMed RFP, June 6, 1997

61. Consortia (10 member corporations) response to CORBAMed RFP, May 30, 1997

62. Materials from Workshops on Components of Computer-based Records sponsored by CPRI, Los Alamos National Laboratory, Health Open Systems and Trials, HCFA, HL7, CORBAMed/OMG and others related to Master Patient Index Services, 1996.

63. MPI to MPI/Networking MPIs Working Group Summary, June 26, 1997.

64. Family Health Outcomes Project, University of California, San Francisco Core Date Element-based Common Patient Identifier Data Element Specifications, February 9, 1997

65. HL7 Special Interest Group: Master Patient Index Mediator (SIGMPI) Mission Statement Document, February 7, 1997.

66. HL7 Special Interest Group: Master Patient Index Mediator (SIGMPI) Presentation by James M. Gabler, HL7 SIG MPI Co-chairperson.

67. "Managing Care: The Role of Enterprise Person Directories" by James M. Gabler, HL7 SIG MPI Co-chairperson.

68. United States Postal Service Electronic Commerce Services presentation documentation from Charles R. Chamberlain, June 1997.

69. John G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol 15, No 11, November 1993.

70. IrisScan, Inc., "IriScan Biometric Human Iris Automatic Identification System Description", August, 26, 1997.

71. Special Healthcare Report, "VA issues 2.5 million ID Cards", Automatic I.D. News, February 1997.

72. Family Health Outcomes Project, University of California, San Francisco Core Date Element-based Common Patient Identifier Data Element Presentation by Dr. Geraldine Oliva, M.D., Ph.D. to NCVHS on June 4, 1997.

73. Director of California Department of Public Health's communication regarding the implementation of Common Data Elements, Marh 21, 1997.

74. F:2 Unique National Patient Identifiers Track, Toward an Electronic Patient Record '97, May 2, 1997

75. Work Group for Electronic Data Interchange (WEDI) "Report to Secretary of US Department of Health and Human Services, July 1992

76. "Computerized Records: A Guide to Security," American Psychiatric Association Resource Document.

77. Joint Commission of Accreditation of Healthcare Organizations (JCAHO) Information Management Standards for Hospital Accreditation 1997

78. Joint Commission of Accreditation of Healthcare Organizations (JCAHO) Quality Control Standards for Laboratory Accreditation Manual 1997.

79. "Digital ID Backgrounder," VeriSign, Inc., December 1996.

80. "For the Record, Protecting Electronic Health Information," National Research

Council, National Academy Press, 1997

81. Lifetime Human Service and Treatment Record Number Document by Edward F. Hernandez, Bureau of Records and Statistics, San Francisco Department of Public Health.

82. "Nomadicity Standards Needs (IISP Need #91) Unique and Anonymous IDs" - Information Infrastructure Planning Panel (IISP)

83. "Statement on the use of the Social Security Number as a National Identifier." presented by Mark H. Epstein, Sc.D, Executive Director, National Association of Health Data Organizations (NADHO) to the Subcommittee on Social Security, U.S. House of Representatives on March 13, 1991

84. Statement of Principles on Information for Health System Reform, NADHO, February 1994.

85. Overview of a Healthcare Information System Architecture Beyond the Computer-based Patient Record.

86. MPI-based Directory Technology by Mary Ellen Buccafurno, Northern Telecom, May 8, 1997.

87. "Confidentiality and Privacy: UNIQUE IDENTIFIERS-HOW TO MAKE IT WORK: BLENDING POLICY AND TECHNOLOGY," CHMIS Conference Transcripts, March 1995

88. "Method of Identifying Individuals in Health Information Systems", Deirdre mulligan, Center for Democracy and Technology, 1995

Acknowledgments

1. Sandy Crank, Associate Commissioner, SSA

2. Dr. Barry Heib, MD., ASTM

3. Dr. Peter Szolovitz, Ph.D., Massachusetts Institute of Technology

4. Dr. Willis H. Ware, RAND

5. Dr. Chris Chute, MD., Mayo Clinic

6. Peter Weagamann, Medical Record Institute

7. William L. McMullen, Mitretek

8. Margaret Amatyakul, Executive Director, CPRI

9. Dr. Gerraldine Oliva, M.D., Ph.D.

10. Teddy Milder, PNP, PHN

11. James M. Gabler, HL7 SIG MPI Co-chair

12. Tim Brinson, CORBAMed, Co-chair

13. Tony Seegar, VAH, Utah.

14. Chaz Kastel, Ralph H. Johnson V.A. Medical Center, Charleston, S.C.

15. Mary Ellen Buccafurno, Northern Telecom

16. Edward F. Hernandez.

17. Derek Wang, SSA

18. Gary Dickinson, Health Data Sciences

19. James P. Brandt, VeriSign

20. Charles R. Chamberlain, USPS

Part Twelve: Author's Biography

Soloman I. Appavu is the President of the Center for Healthcare Automation Ltd., Chicago, Illinois. He has 17 years of healthcare experience. He has served as the Director of Hospital Information Systems and Director of Clinical Information Systems in large metropolitan hospitals. He is currently serving as the Director Financial Control at Cook County Hospital, Chicago, Illinois. He serves as a faculty in national educational programs and conferences. He is active in national healthcare standards and informatics initiatives and holds leadership in technical committees and standards organizations:

1. Chairman, ANSI-HISB Publicity, Education & Information Standing Committee
2. Board Member of American National Standards Institute - Healthcare Informatics Standards Board (ANSI-HISB)
3. Leader, Unique Health Identifier Task Force, ANSI-HISB
4. Track Chair, Unique Patient Identifier, Toward Electronic Patient Record '97.
5. Co-chair, CPRI Work Group on Unique Patient Identifier
6. Member, Education Steering Committee, Healthcare Information and Information Management Systems Society (HIMSS).
7. Technical Committee Member in multiple Standard Developing Organizations (SDOs)
8. Speaker at national conferences and educational programs