

Unique Health Identifier for Individuals

A White Paper

SUMMARY: The Secretary of Health and Human Services (HHS) intends to publish a proposed rule on requirements for a unique health identifier for individuals. These requirements are mandated by law and are part of a process to achieve uniform national health data standards and health information privacy that will support the efficient electronic exchange of specified administrative and financial health care transactions. The Secretary will first publish a notice to discuss the identifier options that have been put forward for consideration and to ask for public comment.

I. General Background

A. Legislation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) outlines a process to achieve uniform national health data standards and health information privacy in the United States. Enacted with the widespread support of the industry and bipartisan support in the Congress, the law requires that the Secretary of Health and Human Services (HHS) adopt standards to support the electronic exchange of a variety of administrative and financial health care transactions. All health plans, health care clearinghouses, and those health care providers who elect to conduct the specified transactions electronically are required to comply with the standards within 2 years of their adoption, except that small health plans are required to comply within 3 years. Among these standards are:

1. Certain uniform transactions and data elements for health claims and equivalent encounter information, claims attachments, health care payment and remittance advice, health plan enrollment and disenrollment, health plan eligibility, health plan premium payments, first report of injury, health claim status, referral certification and authorization, and for coordination of benefits.
2. Unique identifiers for individuals, employers, health plans, and health care providers for use in the health care system.
3. Code sets and classification systems for the data elements of the transactions identified.
4. Security standards for health information.
5. Standards for procedures for the electronic transmission and authentication of signatures with respect to the transactions identified.

Privacy and confidentiality protections for health information play a prominent role in the law as well. The Secretary is required to adopt security standards to safeguard health information, during transmission and while stored in health information systems, to ensure the integrity of the information, and to protect against unauthorized uses and disclosures. Further, the law requires the Secretary to make detailed recommendations to the Congress for protection of individually identifiable health information. These recommendations were delivered to the Congress on September 11, 1997. If the Congress does not enact legislation for health record privacy by August 21, 1999, the law requires the Secretary to issue regulations to protect the privacy of individually identifiable health information transmitted in standard transactions. These regulations must be finalized by February 21, 2000.

The law also specifies steep penalties for misuse of a health identifier and for wrongfully obtaining or

disclosing individually identifiable health information. The penalties, which increase by type of offense, can be as much as \$250,000 and 10 years in prison. More serious offenses are defined as those committed under false pretenses or those committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.

HHS formed five implementation teams to identify and analyze options and propose policies to implement the statutory requirements. Through the publication of several proposed rules in the **Federal Register**, HHS will propose standards for each item required in the legislation.

B. Purpose of The Notice of Intent

There has been considerable consensus on most of the standards that HHS is to adopt. However, opinion on the unique identifier for individuals is deeply divided. Given the level of controversy surrounding the individual identifier, HHS made the decision to proceed cautiously in fulfilling its statutory responsibility to adopt a unique health identifier for individuals for use in the health care system. The notice of intent is the vehicle by which HHS will examine the controversial dimensions of a unique health identifier for individuals, discuss a number of identifier options from which a choice might be made, identify advantages and disadvantages of those options, and request the public to comment. Any subsequent public policy decisions or proposed rules about the unique individual identifier will benefit from the public debate and information gathering elicited by the notice.

Among the areas where comments are solicited are the following:

- What are the major confidentiality and privacy concerns associated with a health identifier for individuals and how should they be resolved? What principles should underlie the choice and implementation of an identifier? What uses should be approved for the health identifier for individuals? What is the relationship of this identifier to legal protection for health information generally?
- What model should be selected for a health identifier for individuals? Are there other viable options that are not discussed in this notice? How should candidate identifiers be evaluated? Are the relevant positive and negative aspects included for the alternatives in this notice? Which alternative do you prefer and which ones should be eliminated from consideration? Why?
- What will it cost both to transition to a new identifier system and to operate it? Who should pay those costs and why? What will the impact be for small providers and, if significant, how can it be mitigated?
- What are the critical implementation issues for a health identifier for individuals and how should they be addressed? For instance: How will the system of authenticating requests and assigning identifiers work on a day-to-day basis? Who will operate the system? What are the infrastructure requirements? How can encryption and other digital security technologies enhance identifier protection? What will the transition process look like?

The notice will also seek comments from the public on additional specific implementation questions in Section IV., Implementation Issues Needing Further Consideration.

C. Future Activities

- 60-day public comment period.
- Analysis of comments on the notice.
- Public hearings conducted by the National Committee on Vital and Health Statistics (NCVHS) in Washington and in different regions of the Nation.

- NCVHS recommendations to Secretary.
- HHS decision to issue a notice of proposed rulemaking or take other action.

II. Identifier for Individuals

A. Need for Unique Identifier for Individuals

HIPAA recognized the unique identifier for individuals as an essential component of administrative simplification. There is evidence that a unique identifier for individuals in the health system would have many benefits, including improved quality of care and reduced administrative costs. Being able to identify an individual uniquely is essential in both the delivery and administration of health care. Today, various health care organizations and insurance companies, integrated delivery systems, health plans, managed care organizations, public programs, clinics, hospitals, physicians, and pharmacies routinely assign identifiers to individuals for use within their systems.

Typically, identifiers differ across organizations, while the delivery and administration of health care traverse organizational boundaries frequently. In its report on computer-based patient records (1991), the Institute of Medicine noted that the increased mobility and aging of our population create pressures for patient records that can manage large amounts of information in different locations and at the same time be easily transferrable among an increasing variety of health care providers. For the vast majority of people today, health records no longer consist of a paper file in a single provider's office. Rather, they consist of many records, some paper but an increasing number electronic, as patients visit multiple providers, primary care providers refer patients to specialists, health plans coordinate benefits with other health plans, providers submit claims and eligibility transactions to multiple health plans, and so forth.

The common practice today is for each provider and plan to use different identifiers for the same individual. Efforts to assure continuity of care, accurate record keeping, effective follow-up and preventive care, prompt payment, and detection of fraud, waste, and abuse all could benefit from the availability of a single unique identifier for individuals with appropriate protections against misuse and unauthorized use outside of health care. A unique identifier is necessary because the constellation of personal attributes commonly used to identify an individual (for example, name, birth date, and sex) is rarely captured in the same manner by each entity in the diverse system of health care. Yet, good care depends on the provider's ability to synthesize information from a variety of sources into an accurate picture of the patient's state of health. The first step in this process is for the proper records to be positively identified. A unique identifier would allow for the rapid and accurate identification of the proper records and their integration for the purpose of providing high quality, patient-focused care.

Having multiple identifiers for the same individual within or across organizations prevents or inhibits timely access to integrated information. Unique identifiers for individuals would facilitate ordering tests and reporting results; posting results, diagnoses, procedures, and observations to charts; updating, maintaining, and retrieving medical records; as well as integrating information across the various internal information systems. For some highly sensitive records (for example, records of mental health diagnoses or treatment, HIV antibody tests, or genetic tests) unique identifiers for individuals would be critical components of administrative procedures designed to protect such information from inadvertent disclosure.

A unique identifier for individuals could serve multiple purposes even within a single health care delivery organization. For some clinical interventions -- for example, blood transfusions, invasive tests or surgery, and medication administration -- a reliable means of identifying the patient is important for safety as well as for record keeping purposes. For example, ensuring safe and effective medication

administration requires integrated information about the drug and dose being ordered, other medications being taken or recently ordered, and known drug allergies. Accurate and efficient integration of this clinical information, sometimes from different systems within one organization, would be assisted by having a unique identifier for individuals associated with each piece of information.

There is considerable support within the health industry for the adoption of a unique identifier for individuals. In a letter to the Secretary dated November 12, 1997, five major standards development organizations and associations that are described as clinical domain experts recommended the prompt adoption of a unique individual identifier. These organizations are: American Nurses Association, Digital Imaging and Communication in Medicine, Health Level Seven, National Association of Chain Drug Stores, and National Council for Prescription Drug Programs. The reasons cited were to reduce administrative workloads and costs, enable faster access to critical health information, and increase efficiency in the exchange of electronic data.

B. Confidentiality and Privacy

Controversy over the adoption of a standard for the unique health identifier for individuals has focused, to a large degree, on privacy concerns. Some of these views contrast sharply with the previous discussion of the value a unique identifier for individuals would have in clinical practice. We should stress that these privacy issues are substantive, not a trivial concern or a public relations matter. For some, privacy threats outweigh any practical benefits of improved patient care or administrative savings. To others, privacy concerns are significant, but can be managed. To some, the status quo poses greater privacy risks. In this section, we review a range of opinions on how privacy and confidentiality issues, including Federal privacy legislation, relate to identifier options. We welcome comments on these issues.

1. Perspectives on the Unique Identifier and Privacy

The Consumer Bill of Rights and Responsibilities, which was published in November 1997 by the President's Quality Commission, underscored the importance of the confidentiality of identifiable health information. The confidentiality right states in part: "Consumers have the right to communicate with health care providers in confidence and to have the confidentiality of their individually identifiable health care information protected..." We welcome comments on whether adoption of a unique health identifier for individuals is congruent with this right. (The complete text of the report is available at <http://www.hcqualitycommission.gov/cborr/consbill.htm>.)

Some believe that threats to privacy are inherent in any unique identifier for individuals. Having different identifiers for the same individual across organizations is sometimes perceived to be protective of individual privacy because potential linkages across data systems are impeded. Having all health care organizations use the same identifier increases the threat to privacy by facilitating unauthorized linkages of information about an individual within and across organizations. This is why some believe that an electronic environment poses greater risks than one that relies on paper records.

Further, if the Social Security number (SSN) were to become the unique health identifier for individuals, some believe that the potential for linkages expands to include not only an individual's medical data but also credit and financial data, employment information, consumer behavior data, and a wide range of other information. The availability and widespread use of the SSN combined with the increasing use of electronic databases and the lack of adequate legal and social controls lend support to these concerns. To some, the SSN is simply unacceptable for identifying health records.

To others, preserving the ability to link health care records with records from other sources using the SSN is essential. The choice of an identifier that is used only in health care could constrain important clinical and public health research that depends on such linking. For example, linkage of health databases and other data sets using a unique individual identifier can assist public health researchers:

- By the linkage of police accident reports and hospital records to evaluate the effectiveness of injury prevention through use of helmets, passive restraints, and airbags.
- By the linkage of environmental or work place exposure records with medical records containing potential health outcomes and worker demographics.

If a unique identifier used only for health care purposes were to be selected, those studies could not be done without a directory for linking the identifier to corresponding SSNs.

In the midst of the differing opinions over what unique identifier might be acceptable and whether it is necessary, it is easy to forget the implications of current practices. Because identifiers differ across organizations, most health care records and transactions contain more elements of identifying information than might be necessary if a single unique identifier were used. Typically, health care records contain a patient's name, gender, address, phone number, birth date, SSN, health insurance number, employer, and relationships to other family members. A combination of several of these data items is often necessary to ensure a correct match between the records and a particular individual. In effect, a medical record or transaction bearing merely a person's name and address may make the information "open" to anyone who deliberately or accidentally comes in contact with it. Ironically, this use of personal information for matching people and records generates little controversy, despite the lack of security standards and privacy protections in place today.

In addition, some believe that protection of health information from inadvertent or unauthorized disclosure would become easier with a unique individual identifier that is used for health care, but not for other purposes. Such an identifier would be used in a similar manner to the way that HIV testing is often conducted anonymously, by assigning an individual a number that is not otherwise known or used. This number, which is used to track and retrieve the test result, cannot easily be used to identify the individual, whereas name and other identifiers could be. A test result bearing only a protected number cannot be associated easily with an individual.

From this perspective, an identifier that could replace other items of identifying information and that would be used only in health care might yield greater privacy protection than alternatives that do not share these properties. Other such properties have been suggested. A check digit that could be used to validate an identifier might further reduce the need for other identifying information. An identifier with no embedded intelligence (e.g., initials or a location code) would be more protective than one containing intelligence. A longer identifier would be less easily transcribed or remembered than a shorter one. Encryption of an identifier under controlled conditions might add protection. A decentralized method of issuing identifiers that required no central database would offer other protections. We welcome comments on these and other properties of identifiers that would contribute to privacy protection.

2. Importance of Privacy Legislation

Regardless of possibilities for protecting medical information by using a unique health identifier for individuals and by applying the security safeguards required by HIPAA, some argue that HHS should not select a unique health identifier for individuals until the Federal privacy legislation required by HIPAA has been enacted. In the meantime, of course, identification of individuals' medical records and transactions will continue, even though the methods are costly and burdensome and may themselves be

a threat to privacy.

We welcome comments on what the major confidentiality and privacy concerns associated with a unique health identifier for individuals are and how they should be resolved.

3. [NCVHS Recommendation](#)

The National Committee on Vital and Health Statistics (NCVHS), which was given a special role by HIPAA to advise the Secretary on standards issues, itself recommended that HHS not adopt a standard for a unique identifier for individuals until after privacy legislation is enacted. The NCVHS stated that "...it would be unwise and premature to proceed to select and implement such an identifier in the absence of legislation to assure the confidentiality of individually identifiable health information and to preserve an individual's right to privacy."

The NCVHS outlined three concerns. First, it noted that the selection of a unique health identifier for individuals will become the focus of tremendous public attention and interest, far beyond that afforded to other health privacy decisions. It concluded that no choice should be made without more public notice, hearings, and comment. Second, it concluded that, until new Federal privacy law adequately protects health record privacy, it is not possible to make a sufficiently informed choice about an identification number or procedure. The degree of formal legal protection in such a law will have a major influence on both the decision itself and the public acceptance of that decision. Indeed, passage of a comprehensive health privacy law may make the choice of an identifier easier and less threatening to privacy. Finally, the NCVHS believed that a unique health identifier for individuals could not be protected from misuses under current law, notwithstanding the criminal penalties enacted in HIPAA. [The full text of the NCVHS recommendation is available at <http://ncvhs.hhs.gov/uhid.htm>.]

The NCVHS is conducting public hearings to explore these issues during 1998. Information about these hearings will be posted on the NCVHS website at <http://ncvhs.hhs.gov/>.

C. Approved Uses of an Identifier for Individuals

In addition to the HIPAA requirements for health information security and privacy, Congress included provisions in HIPAA that relate directly to the individual identifier and constrain its use. HIPAA directs the Secretary of HHS to adopt "standards providing for a standard unique health identifier for each individual ... for use in the health care system." HIPAA goes on to say that the standards "shall specify the purposes for which a unique health identifier may be used." Therefore, in any proposed rule to adopt a particular identifier, HHS would be obligated to specify the purposes for which the identifier would be required, permitted, and prohibited. The notice raises some of these issues to elicit your comments.

HIPAA's language suggests that uses of the individual identifier outside the health care system could be prohibited, and that HHS could designate that such uses would be an offense subject to the penalties outlined in HIPAA. This leaves open the question of what other uses within the health care system might be approved or disapproved as well as what the boundaries of the health care system are. Certain approved uses can be derived directly from HIPAA. HIPAA requires use of the unique individual identifier in administrative and financial health transactions adopted by the Secretary under HIPAA authority. Thus, the identifier no doubt would be used in health care treatment, payment, and associated administrative and financial activities.

While HIPAA mandates the adoption of a standard unique identifier for use in the health care system, it does not mandate its use for purposes other than the transactions listed in the statute. There are many

ways that the identifier could lawfully come into use for such other purposes. For example, such purposes could be permitted (but not mandated) by listing them among the “lawful uses” HHS is required to publish with the identifier. Use of the identifier could be required by other programs, for example, by an accreditation organization in its standards for quality assurance record keeping, or by the FDA for reporting adverse drug reactions. These additional potential uses of the identifier should be taken into account in considering the identifier alternatives.

Similarly, in a regulation proposed on May 7, 1998, in 63FR25320, the unique identifier for health care providers will be required in the administrative and financial transactions adopted under HIPAA and will be permitted (but not required) to be used for other purposes.

Limiting the uses of the unique identifier for individuals to purposes related to health care could be more important than for the identifier for health care providers. Other statements of policy offer additional specificity on the boundaries of the health care system. The President’s Quality Commission described the uses and disclosures of individually identifiable health care information that were consistent with the right to confidentiality and could be made without direct patient consent. These included uses and disclosures for:

- Health purposes, including provision of health care, payment for services, peer review, health promotion, disease management, and quality assurance.
- When there is a clear legal basis for the disclosure in very limited circumstances; medical or health care research for which an institutional review board has determined anonymous records will not suffice, investigation of health care fraud, and public health reporting.

The Secretary’s recommendations for Federal privacy legislation would authorize uses of individually identifiable health information without direct patient consent for:

- Health care and payment.
- Health oversight of many types, including oversight by law enforcement, government agencies investigating or paying for health care, professional licensure and discipline systems, regulators such as insurance commissioners, and accreditation, standard-setting, and quality review bodies.
- Public health, including public health surveillance.
- Health research, under certain limited conditions (for example, with approval of an institutional review board).
- Emergency purposes.
- Health data collection by state agencies.

Both the President’s Quality Commission and the Secretary recognized that we must take care not to draw the boundaries of the health care system and permissible uses for the unique identifier too narrowly. They recognized that quality assurance, health research, and public health reporting, for example, are within the realm of the health care system and ought to be permitted to use the unique identifier.

We will welcome public comment on the purposes for which a unique health identifier for individuals could be used and whether limits should be placed on such use. If so, what should the limits be?

D. Criteria for Evaluation of Candidate Identifiers

Much has been published about the need for a unique identifier for individuals and the criteria that should be considered in selecting an identifier. While different authors bring different perspectives to

these topics, there is also some overlap, as would be expected. A general discussion of some of the published or frequently discussed criteria is included below. There is not consensus on the criteria that should guide the selection of a unique identifier for individuals. These criteria are presented to stimulate thought about the identifier characteristics.

1. Standard Guide for Properties of a Universal Healthcare Identifier (UHID)

The American Society for Testing and Materials (ASTM), a standards development organization accredited by the American National Standards Institute, has published the *Standard Guide for Properties of a Universal Healthcare Identifier (UHID)*, hereafter referred to as the Standard Guide. The Standard Guide and its criteria will be referenced in the following discussion of each proposal. The Standard Guide provides 30 criteria against which one may evaluate candidate identifiers and a sample UHID, which illustrates the use of the criteria. The 30 criteria are designed to support four basic functions of a universal health care identifier in the population of the United States. The functions are: (a) Positive identification of patients when clinical care is rendered, (b) Automated linkage of various computer-based records on the same patient for the creation of lifelong electronic health care files, (c) Provision of a mechanism to support data security for the protection of privileged clinical information (does not attempt to address all safety concerns, however), and (d) Use of technology for patient records handling to keep health care operating costs at a minimum.

The Standard Guide also discusses the need for a temporary patient identifier when the universal health identifier is not available; for example, emergency care of unconscious patients, care provided to infants when a responsible informed adult is not present, or care being provided when a significant language barrier exists. During public discussions of the unique identifiers, participants have stressed that the unique health identifier should be available at birth.

The 30 criteria are:

- Accessible (available when required).
- Assignable (assign when needed by trusted authority after properly authenticated request).
- Atomic (single data item--no subelements having meaning).
- Concise (as short as possible).
- Content-free (no dependence on possibly changing or unknown information).
- Controllable (only trusted authorities have access to linkages between encrypted and non-encrypted identifiers).
- Cost-effective (maximum functionality with minimum investment to create and maintain).
- Deployable (implementable using a variety of technologies).
- Disidentifiable (possible to create a number of encrypted identifiers with same properties).
- Focused (created and maintained solely for supporting health care--form, usage, and policies not influenced by other activities).
- Governed (has entity responsible for overseeing system--determines policies, manages trusted authorities, and ensures proper and effective support for health care).
- Identifiable (possible to identify the person with such properties as name, birth date, sex, etc, by associating these with the identifier).
- Incremental (capable of being phased in).
- Linkable (can link health records together in both automated and manual systems).
- Longevity (designed to function for foreseeable future with no known limitations).
- Mappable (able to create bidirectional linkages between new and existing identifiers during incremental implementation of a new identifier).
- Mergeable (can merge duplicate identifiers to apply to the same individual).
- Networked (supported by a network that makes services available universally).

- Permanent (never to be reassigned, even after a holder's death).
- Public (meant to be an open data item--person can reveal it).
- Repository-based (secure, permanent repository exists to support functions).
- Retroactive (can assign identifiers to all existing individuals when system is implemented).
- Secure (can encrypt and decrypt securely).
- Splittable (able to assign new identifier to one or both people if the same identifier is assigned to two people).
- Standard (compatible if possible with existing or emerging standards).
- Unambiguous (minimizes risk of misinterpretation such as confusing number zero with letter O).
- Unique (identifies one and only one individual).
- Universal (able to support every living person for the foreseeable future).
- Usable (processable by both manual and automated means).
- Verifiable (can determine validity without additional information).

Use of the Standard Guide helps to ensure that all proposals for an individual identifier receive scrutiny against the same set of criteria covering a broad range of considerations. Several noteworthy aspects of the relationship between the proposals described in this document and the various evaluation criteria hamper the ability to apply meaningful numeric "scores." Some of the criteria (such as atomic--meaning a single data item without subelements) are relevant to a unique identifier, while others (such as mappable-- meaning possible to create bidirectional linkages between identifiers during incremental implementation) describe a system for maintenance or implementation. However, most of the proposals for an individual identifier provided only a concept of the identifier itself and did not include a proposed infrastructure or trusted authority to establish or maintain the system.

The Standard Guide provides a system for assigning a numerical score to each of the 30 criteria, but provides no method for weighting the relative importance of the criteria. Most of the proposals fully or partially met a large number of the criteria. However, among the proposals considered, only one included an analysis of both the identifier and the infrastructure needed to implement and maintain it. Some of the proposals would not ensure a unique identifier for each individual. Some of the proposals are not identifiers at all, but rather are systems of identification or maintenance of an infrastructure for identification. For these reasons, numeric scoring of each criterion may not be the most valuable way to use the Standard Guide. Nevertheless, the criteria served as a baseline set of functions against which all proposals were considered, and both positive and negative aspects were identified and compared.

2. Institute of Medicine's Committee on Regional Health Data Networks

Six qualities of an ideal identifier were identified by the Institute of Medicine's Committee on Regional Health Data Networks.

- It must be able to transition easily from the present record-keeping environment.
- It must have error-control features.
- It should have separate identification elements (to indicate who the individual is) and authentication elements (to allow validation of identity with high confidence levels using parameters other than the identification elements).
- It must work in any circumstance in which health care services are provided.
- It must work anywhere and in any provider's facilities.
- It must help minimize the opportunities for crime and abuse.

3. Practicality and Cost Effectiveness

Representatives from all segments of the health system have emphasized that practicality and cost effectiveness must be given careful consideration in selection of a unique identifier for individuals.

- In order for a unique individual identifier to be effective, every individual should have an identifier that applies only to that individual and that does not change over time.
- An identifier or identifier system that is not practical to implement or that does not meet the requirements of administrative simplification must be deemed unacceptable.
- The costs of implementation and use of the identifier must be within an acceptable range. To determine whether costs are acceptable, we must consider costs for all the participants in the health care setting -- for patients, health care providers, health plans, State and local governments, and the Federal Government.

4. Privacy Principles

As noted earlier, privacy considerations are key in choosing the identifier. There are several criteria that might be applied in determining whether a particular identifier helps to serve the privacy interests of individuals. In order to stimulate thought and comment on the relationship between privacy and the identifier, some criteria that have been discussed in privacy studies are presented:

- Privacy protection governing use and disclosure of the underlying data attached to the identifier, in the form of legal, technical, and administrative controls, is essential.
- The identifier should not contain substantive information about the individual.
- The identifier must not be used to establish a single national data base of all health records.
- The identifier must not be used as a basis for a national identity card system.
- There must be prohibitions on use of the identifier for purposes outside of health.

Many of the criteria that might be used to evaluate candidate identifiers can be summarized as relating to practicality, cost effectiveness, or privacy. Privacy must be balanced with practicality and cost. An identifier that protects privacy absolutely may rely on a technology that is neither practical to implement nor cost effective. An identifier that is the least expensive or simplest to implement may pose unacceptable privacy risks. The challenge is to find an identifier option that achieves an appropriate balance among privacy, practicality, and cost.

III. The Candidate Identifiers

The American National Standards Institute's (ANSI) Healthcare Informatics Standards Board (HISB) prepared an inventory of existing healthcare informatics standards to assist the Secretary with adopting standards. Information was collected by ANSI HISB from accredited standards development organizations, other organizations, and government agencies. The inventory included a discussion of standards for a unique identifier for individuals. It reported that ASTM was the only standards development organization with a published standard, the Standard Guide, on this topic and listed ASTM's Sample UHID as a proposed identifier. It also listed six other candidate options which are "frequently discussed by industry experts." The six options are:

- Social Security Number (SSN), including the proposal of the Computer-based Patient Record Institute (CPRI).
- Biometric Identifiers.
- Directory Service.
- Personal Immutable Properties.
- Patient Identification System based on existing Medical Record Number and Practitioner Prefix.

- Public Key-Private Key Cryptography Method.

Additional proposals are also addressed in this paper.

Overall, the proposals for unique identifiers for individuals fall into four general classes.

- Unique Identifier Proposals Not Based on the SSN.
- Unique Identifier Proposals Based on the SSN.
- Proposals That Do Not Require a Universal, Unique Identifier.

HIPAA requires that the Secretary of HHS adopt a standard for a unique identifier for each individual for use in the health care system. In the interest of promoting a full and complete discussion of all options, we present here several options that do not include a unique identifier but that may nevertheless allow each individual to be accurately identified in the health care system.

- Hybrid Proposals.

A. The SSN and Enumeration Process of the Social Security Administration (SSA)

Many of the proposals involve either the SSN, SSA's enumeration process, or both. The following background relates to some or all of these proposals and includes discussion of information about the use of the SSN as a personal identifier, improvements in the SSA enumeration process that have been undertaken, other needed improvements, and the costs of such improvements.

1. Information About the Use of the SSN as a Personal Identifier

The SSA has always taken the position that the SSN is not a personal identifier. When the Social Security law was passed in 1935, the SSN was called the Social Security Account Number and was meant to identify the account, not the person. However, in practice, the SSN has been adopted for numerous identification purposes outside of the Social Security system. In 1943, President Franklin D. Roosevelt signed an Executive Order requiring Federal agencies to use the SSN as an identifier for any new record systems. The Department of Defense used the SSN as a military identification number during World War II and adopted it officially in 1967 as an Armed Services personnel identifier.

In 1961, the Civil Service Commission adopted the SSN as an official Federal employee identifier, and in 1962 the Internal Revenue Service adopted it as the taxpayer identification number. In the 1960s, the Treasury Department required buyers of Series H savings bonds to provide their SSNs and again in the 1970s required it for the purchase of Series E savings bonds. The SSN was selected in the 1960s as the Medicare health insurance number, with an alphabetic character appended to designate the beneficiary's relationship to the wage earner on whom benefits are based.

In 1970, financial institutions were required by law to obtain SSNs of all their customers. Although the Privacy Act of 1974 prohibited States from using the SSN without congressional authority, it allowed those already using it to continue. Then, the Tax Reform Act of 1976 authorized States to use the SSN for State and local tax authorities, welfare systems, driver's license systems, departments of motor vehicles, and for finding parents who were delinquent in child support payments. Later laws required or permitted States to require SSNs for participation in school lunch programs, Food Stamp programs, and numerous other programs. Placement of the SSN on State drivers licenses is required by the year 2000 under a 1996 immigration reform provision.

There are few prohibitions against use of the SSN in the private sector. Educational institutions frequently use the SSN as a student identifier, and the National Student Loan Data System has required the SSN of the borrower since 1989. Many health care providers also use the SSN to identify patients. Many private health plans use the SSN to identify subscribers and, to a lesser extent, dependents. Individuals are now indexed by their SSN in a number of databases with routine linkages and data exchange among them. The SSN is in such extraordinarily wide use as to be a *de facto* personal identifier. With appropriate privacy and confidentiality protections mandated in HIPAA legislation, the choice of using a unique identifier associated with the SSN would facilitate the potential linkage of medical records with administrative databases, as needed for public health or clinical research. Although the SSN is widely used as a health identifier in many health systems, legislation would likely be required for the SSN to become the unique identifier for individuals envisioned by HIPAA. This is because when an organization independently decides to use the SSN as an individual identifier, individuals may elect to withhold their SSN. However, when the use of the SSN is statutorily mandated, as is possible under HIPAA, the Social Security Act should be modified to specifically authorize the SSN for that use.

2. Improvements in the SSA Enumeration Process

The SSA has taken steps to overcome problematic aspects of the SSN that stem from the current system's lack of both a strategy for systematic assignment to every person and a means to authenticate a person's identity. The SSA has improved its process to verify the identity of the person receiving an SSN. Before 1971, the issuance of SSNs was based on information provided by the individual. Starting in 1971, some applicants had to document evidence of age, identity, and alien status. In 1974, the SSA started recording when a non-work SSN had been issued to an alien and reported this to the Immigration and Naturalization Service. Beginning on May 15, 1978, applicants for SSNs have had to document (using documents such as birth certificate or driver's license) age, identity, and citizenship or alien status. If the applicant is at least 18 years old, a personal interview is conducted to determine if the person has had an SSN before. Additional verification is performed, such as contacting the State Bureau of Vital Statistics to verify the existence of a birth certificate, conducting a search for a death certificate or verifying Immigration and Naturalization documents presented by the applicant. Currently, the verification process is based on a combination of personal data such as name, date and place of birth, sex, mother's maiden name, and father's name. These data elements are also used to screen the SSA database for any previous issuance to the person. The SSA reported to Congress in 1997 that its SSN database is highly accurate and allows assignment of an SSN within 24 hours if there are no questions about the data.

3. Other Needed Improvements

Beginning with tax returns filed 1/1/98 or later, the SSNs of all dependents claimed by a taxpayer must be included on the tax return. Thus a child could need an SSN during the first year of life. SSA's "Enumeration at Birth" process allows a parent to apply for an SSN for his/her newborn as part of the State's birth registration process. The State sends to SSA the data needed to assign an SSN and issue a card. About half of the original Social Security cards issued in fiscal years 1993-1994 used the "Enumeration at Birth" process. The addition of California in the process added an estimated 15 percent for fiscal year 1995. All 50 States, as well as New York City, Washington, DC, and Puerto Rico, now participate in this process.

In 1988 and again in 1991, the HHS Office of Inspector General cited major weaknesses in the birth certificate issuance process that hampered the ability of both Federal and State user agencies to rely on birth certificates retrospectively for identity. Among the problems cited were the use of false birth certificates as "breeder documents" to create false identities. The SSA defined breeder documents as

those "... that are used to obtain other documents used for identity: for example, a birth certificate is used to obtain a drivers license, which is then used as an identity document." The HHS Office of Inspector General also cited as problems the many different versions of birth certificate forms that are used, and open access with lax physical security for vital records.

All of the proposals for a health care identifier that depend on the SSN or the SSA would benefit from further improvements in the process for issuing and maintaining both SSNs and birth certificates. An improved process could begin with a newborn patient in the birth hospital or other health care provider; at once the proper authorities would assign a birth certificate number, assign an SSN, and assign the health identifier. Such a process would permit the longitudinal patient record to begin at the initial health care encounter. Health care providers that deliver newborns in non-hospital settings would need to have a method to access this system and report to it when necessary. Improved accuracy in identification and reductions in fraud from a process linking birth registration and SSN issuance would benefit vital records agencies, SSA, and the public. These processes for assigning identifiers at birth would have to be supplemented with procedures to verify identities and issue numbers to individuals (for example, immigrants) whose enumeration would not occur at birth. The legislation that would be necessary to involve the SSA in this process would need to allow for these improvements.

4. The Costs of Improving SSA Enumeration

In relative terms, building upon an existing system, such as that administered by the SSA, should be less costly than creating an infrastructure to administer an entirely new identifier system. Nevertheless, proposals that require substantial investments by the SSA to improve its processes must address SSA's costs for those changes. The need to improve the existing SSN system by eliminating duplicate numbers and re-verifying the identities of SSN holders is well established and independent of proposals to use SSA as the trusted authority for issuance of a unique health identifier. The term "trusted authority" as used in this document refers to the authority that will have the responsibility of administering a unique health identifier system.

As noted above, some of the needed improvements began several years ago. The SSNs that were assigned at birth using the enumeration process described earlier would not need to be changed or re-verified, and health identifiers could be issued immediately to people whose SSNs were assigned under the improved processes.

At the request of the Congress, SSA reported recently that, based on fiscal year 1996 data, verifying the identities of all SSN holders and reissuing new cards would have a basic minimum cost of about \$3.9 billion. Additional estimates (up to \$9.3 billion) were given if the process included new security features in the cards. The report did not attempt to estimate possible related costs, such as special processing for very young and very old number holders, those in rural locations, or those outside the United States.

If the SSA were to undertake the re-validation and re-issuance project in order to overcome the current limitations of the SSN, a unique health identifier issuance and maintenance system could benefit from being part of the process. If the SSA were to incur the cost of re-validation and re-issuance, the additional effort to issue a health identifier could be incorporated into the process at the earliest planning stages, and the costs for this process certainly would be smaller than instituting a new system to issue and administer such identifiers.

Improvements to the SSN and to SSA's enumeration process should yield benefits for other activities such as immigration reform and welfare fraud reform. It might be reasonable, therefore, if the improvements were undertaken in connection with SSA's role as trusted authority for issuance of a

health identifier for individuals, to apportion the cost of the improvements across all the agencies that would benefit from them.

B. Unique Identifier Proposals Based on the SSN

1. The Unenhanced SSN

Description This option was listed in the ANSI HISB inventory. The SSN is described in section III.A., above. The SSN is commonly used as an identifier in current health care systems. For this reason, it would be the least costly identifier to implement.

Positive Aspects

- The SSN is readily available to most of the public.
- The cost of implementing the unique health identifier for individuals would be minimized, because many data systems already capture the SSN or use it as a key identifier, and these would not have to be modified.
- The SSN is the current *de facto* identifier. People are accustomed to using their SSN as an identifier in a number of circumstances and would not be required to adjust to change.
- Prospectively, the SSN has good potential for serving as an accurate, unique identifier for most individuals enumerated under the new processes discussed above.
- The Government would bear the cost without having to create a new system.

Negative Aspects

- SSNs have no check digit feature. A check digit is the result obtained by applying an algorithm to a number, such as the SSN or other identifier, to detect keying or transmission errors. Refer to Section IV.D. for further discussion of check digits. One of the major difficulties identified by systems using SSNs is the frequent transposition of numbers during data entry.
- SSNs would not provide for the universe of patients, because some people are not eligible for SSNs and others choose not to obtain one. A mechanism to assign substitute numbers without duplication would need to be created.
- The same SSN is sometimes erroneously used by more than one person.
- Some people legitimately have more than one SSN. The SSA will assign multiple SSNs to a person in certain circumstances, for example, when a person is being disadvantaged by the misuse of his/her SSN, or when the person is being harassed, abused or endangered and his/her SSN played a role in the harassment, abuse or life endangerment. The SSA cross references these multiple SSNs.
- In the event that a person needs health care but cannot give the SSN to the provider, a mechanism for issuing a temporary identifier, and later merging it with SSN identification, would have to be created.
- There are no legal requirements for the many non-Federal users of SSNs as identifiers to keep the number confidential or to limit its use. Protection of the SSN as a health care identifier would be unenforceable.
- A mechanism for health care providers to verify the authenticity of an SSN when it is presented as evidence of identity would need to be created.
- The SSN is not under control of the health care industry, and changes that may be made to benefit one of the many other uses of the SSN may not be beneficial for health care.
- SSNs are easy to counterfeit because allowable entries are well known. Because SSNs are so widely used, obtaining and using someone else's number is relatively easy. This could affect the

accuracy of records linked using this identifier.

- The Medicare identifier currently consists of the SSN of the wage earner on whom benefits are based, plus a suffix to designate the beneficiary's relationship to the wage earner. People who receive benefits based on a spouse's earnings are identified by the spouse's SSN (plus a suffix) rather than their own. The use of the wage earner's SSN could cause a commingling of medical records that are linked based on SSNs.
- SSNs are not available at birth for use by the birth hospital and no system is available for providing temporary SSNs.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in the areas of being focused for health care (created and maintained solely to support health care), for being unique (identifying one and only one person), and for being able to merge or split identifiers (to correct for duplicates) when necessary. Some of the positive aspects of this proposal as revealed by the ASTM criteria relative to other proposals were in the areas of accessibility, content free, and cost effectiveness.

Some of the negative aspects exist primarily with the SSNs that were issued before the improvements in the SSA processes were made. These will be improved or corrected as the proportion of SSN holders who are enumerated under the new procedures increases. However, this may not happen quickly enough to meet the needs for a health identifier for individuals. Some of the other problems are addressed by ongoing or proposed improvements in SSA's enumeration process. Whether these improvements will be made is not known; even if they are, some aspects of using the unenhanced SSN remain problematic.

2. Proposal of The Computer-based Patient Record Institute (CPRI)

In 1993, CPRI published a position paper recommending that the SSN, with modifications in the number and the process for issuing it, be adopted as a "universal patient identifier." In September 1996, CPRI published an *Action Plan for Implementing a Unique Health Identifier*, Version 1.0, hereafter referred to as the Action Plan, which gave further detail on their proposal. The CPRI proposed an identifier based on the SSN, with the addition of a check digit. Many people know only this component of the CPRI proposal; however, the proposal also includes the following improvements and enhancements that would affect the utility of the SSN as a health identifier:

- Enact legislation to fund and task the SSA to add a check digit to the SSN and modify the process of issuing SSNs so it can be used as the unique health identifier. For example, the Action Plan states,

There must be increased funding and specific tasking of the SSA to clean up existing duplication, multiple assignments, and other errors. ... In addition, there must be legislation permitting the use of SSNs for health identification purposes. There must also be a mechanism whereby identifiers can be assigned to those without an SSN. Finally there must be an authentication algorithm used to establish the identity and authority of the organization requesting a number.

- Enact Federal preemptive legislation to provide uniform protection of the confidentiality of health information, as called for in HIPAA.
- Develop and promote a public education program outlining the importance of a unique health identifier and describing how access to individually identifiable health information will be protected and controlled.

Positive Aspects

Because of its reliance on the SSN, the CPRI proposal offers a practical solution that would require a minimum amount of change in current health care databases. It brings benefits of cost, ease, and time to implement when compared with candidates that would implement a completely new health identifier.

- The addition of a check digit may be a valuable incremental improvement to the SSN (but would increase cost and affect formats in systems now using the SSN).
- The enhancements that are a part of the CPRI proposal would provide greater privacy protections without the cost of an entirely new identifier system.

Negative Aspects

- Many of the negative aspects of the Unenhanced SSN (for example, no authenticating feature, Medicare ID of wage earner used, no mechanism for issuing temporary SSNs) carry over to this proposal due to their similarities.
- The referenced changes to the SSN issuance process are not detailed in the proposal, but would be significant, and the time, effort, and cost to make the changes have not been quantified.
- The changes to expand and improve the issuance process and re-verify SSNs to clean up errors, as specified in the Action Plan, would make the proposal very costly.
- It is unclear how the proposed legislation could or should protect health information identified by the SSN from being linked with other information systems that already use the SSN as the basic identifier.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in the areas of being focused for health care (created and maintained solely to support health care), for being unique (identifying one and only one person), and for being cost effective. Many of the aspects of this proposal, as revealed by the ASTM criteria, were positive relative to others, but depended on the enhancements that were outlined generally in the proposal.

3. Alternate to SSN Identifier

Description

This proposal is related to the use of the SSN as the health care identifier. One suggested approach to address privacy concerns with the SSN or the CPRI proposal is to use the SSN as the health identifier for those individuals to whom it is acceptable, but offer an alternate identifier to others. Individuals who have concerns over linkage of their health information with other information already linked by the SSN, could receive a permanent, unique, alternate 9-position identifier. The alternate identifier would not be the same as any current or future SSN. This modification of the SSN proposal would be restricted to the limited number of such alternate numbers available.

Positive Aspects

- Since the alternate identifier would be the same length as the SSN, it could be used in any record structures that carry the SSN.

Negative Aspects

- A potential stigma could be attached to the alternate identifier -- a request for the identifier might be interpreted to mean that the individual has something to hide.
- Additional infrastructure would be required to assign the alternate identifier (ensuring, for

example, that duplicate numbers are not assigned). This would increase the complexity and cost, compared to the proposal for the unenhanced SSN.

- We anticipate that, given the choice, significant numbers of individuals would request the alternate identifier. If the numbers of individuals became too large, the alternate identifier might be required to have one or more alphanumeric characters to handle the increased number of identifiers needed. This, in turn, would likely require changes to data systems, including the internal systems maintained by providers and plans.

Application of the ASTM criteria revealed similar negative aspects of this proposal to others based on the SSN. One difference is in the area of being public (able to be revealed to any person or organization by those who would not want to reveal their SSN). Some of the positive aspects of this proposal as revealed by the ASTM criteria relative to other proposals were in the areas of accessibility, content free, and cost effectiveness.

4. The Computed Healthcare Identifier (CHID)

Description

The CHID proposal provides an alternative to using the SSN. Under this proposal, a new identifier would be computed from the SSN. The proposal would not require changes in SSNs or in SSA's processes, therefore its cost could be lower than that of the CPRI proposal. Assignment of this identifier would be accomplished by health care providers or health plans. During enumeration, each validated health plan and health care provider would be provided a standard encryption algorithm for the purpose of converting a patient's existing SSN into another, private number. The proposed algorithm would perform a one-way mathematical function that is significantly easier to perform in a forward direction than in the opposite, or inverse, direction. A one-way function is sometimes called a trap-door algorithm because, like falling through a trap door, a one-way function is a process that is easy to do but very difficult or even impossible to undo. As an illustration, multiplying four or five three-digit prime numbers together is the mathematical equivalent of falling through the trap door--it is easy to do. It is quite a different matter, however, to take the huge number resulting from that multiplication and calculate backwards to reveal the original four or five numbers. That would be the mathematical equivalent of un-falling through the trap door--it is very hard to do. With a high speed computer it might be possible to compute a one-way function in a fraction of a second, but to compute its inverse could take many years.

Under this proposal, the plan or provider would apply a trap door algorithm to a patient's SSN to compute a new unique health identification number. Since the identical algorithm would be used by all plans and providers, the resulting Computed Healthcare Identifier (CHID) for a specific individual would always be the same and would be used to identify all of that individual's health records. The number would contain check digits that could be used to distinguish valid from invalid numbers.

Unique temporary numbers or identifiers for people ineligible for an SSN would be issued on demand by a health care provider or plan from a national computer system accessible from modems and the Internet. Such identifiers would be indistinguishable from the CHID. Temporary numbers would be issued from the domain of numbers that cannot be computed from a valid SSN. If necessary, the SSA would be asked to set aside a range of SSNs for this purpose and agree never to assign them. This proposal has not been piloted, and no cost estimates are available.

Positive Aspects

- The proposal would not involve the SSA or require any changes in the current process of assigning SSNs, although it would benefit from any improvements the SSA makes in its enumeration system over time, as described above.
- The CHID would be guaranteed mathematically to be unique. The "trap door" algorithm, which would be used to generate the CHID from the SSN, is one that is irreversible (the mathematical process could not be reversed to derive SSN from CHID), thereby impeding attempts to calculate the SSN from the computed identifier.
- The linking of the SSN and computed health identifiers for purposes other than health care or other authorized uses could be prohibited by regulation. Thus, health records could not be linked easily with other information using the SSN as the identifier, a major drawback of using the SSN itself as the identifier.
- The CHID would be less expensive to implement than a system to create a totally new number, although no cost estimates are available. The new number that would be computed from, but not linkable back to, the SSN would require a relatively small expense to taxpayers to distribute the encryption keys. The identifiers would be distributed by plans and providers as needed.
- The CHID could address privacy concerns because it makes linkage to other records using the SSN more difficult.
- Severe criminal penalties exist in current law for unauthorized uses of any health identifier; misuse of the algorithm used to create the numbers could be brought under the same penalty by regulation.
- The infrastructure would be smaller than that required for a new trusted authority to issue and administer a totally new identifier.
- The CHID can be validated with a check digit program.

Negative Aspects

- Since this identifier is based on the SSN, many of the current problems with SSNs would not be addressed unless and until the SSA re-verifies the SSNs.
- Because the algorithm would have wide distribution, it is likely to become publicly known within some relatively short period despite legal sanctions against disclosure, and thereafter it would be a relatively simple matter to compute the health identifier from an individual's SSN.
- Anyone with access to the algorithm who wanted to link the health care identifier with the SSN could, theoretically, take the one billion 9-digit numbers that include all potential SSNs, apply the algorithm, and generate a database of all health identifiers, each linked to its corresponding SSN.
- No infrastructure currently exists to support appropriate linkages of encrypted versions of the CHID back to the original CHID.
- The cost to the industry to modify its systems and add an identifier that is longer than identifiers commonly in use, most likely 16 characters, would be significant.
- An infrastructure would be required to manage temporary identifiers and identifiers for those individuals who have no SSN. Although this would be smaller than the infrastructure required for many other proposals, its cost could still be significant.

Application of the ASTM criteria reflected problematic areas similar to those of the use of the SSN itself--in the areas related to being governed (having an entity oversee and manage the system), such as mergeable and splittable (to correct for duplicates, and in being unique (identifying one and only one person). Some of the positive aspects of this proposal, as revealed by the ASTM criteria relative to other proposals, were in the areas of accessibility, content free, cost effectiveness, and being focused for health care (created and maintained solely to support health care).

C. Unique Identifier Proposals Not Based on the SSN

1. The ASTM Sample UHID

Description

The UHID provided as a sample in the Standard Guide is designed with a length up to 29 characters. The number is constructed from four parts: (a) a 16-digit sequential number that identifies an individual uniquely, (b) a delimiter (defined as a single character, such as a period, that denotes the boundary between two digits or characters) that separates the 16-digit number from the check digits and encryption scheme identifier that follow, (c) 6 check digits, and (d) a 6-digit encryption scheme identifier, if the number has been encrypted. If the UHID does not need to be encrypted, the last six digits can be valued as "000000" or omitted entirely. Leading zeros of the 16-digit sequential number may also be omitted to produce a shorter identifier. The proposal did not describe the Sample UHID's implementation. One of the authors of the proposal suggested it should be a simple implementation, with a small staff operating one computer to assign the numbers.

Positive Aspects

- This proposal meets the requirement of HIPAA for a standard, unique health identifier for each individual.
- It incorporates check digit and encryption capabilities.
- It could restrict the identifier to health care and other desirable uses that can be protected with legislation.

Negative Aspects

- The cost to the industry to modify its systems and add another, longer identifier would be significant.
- As a new number, it would require new or additional infrastructure support to issue and maintain it. Establishing such a new infrastructure for national implementation could be prohibitively expensive and would need to be weighed against the advantages.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in the areas of being governed because of the simple plan described for a small administrative staff and, therefore, for being able to merge or split identifiers (to correct for duplicates) when necessary at a national level. The length of the UHID is also a negative aspect when considering concise (as short as possible) and cost-effective features. Some of the positive aspects of this proposal, as revealed by the ASTM criteria relative to other proposals, were in the areas of accessibility, able to be public, and content free.

2. Biometric Identifiers

Description

The ANSI HISB Inventory of Standards described biometric identifiers as a class of proposals, rather than an individual one, and defined them as sophisticated methods of biometric identification. Biometric identifiers are based on unique physical attributes, including fingerprints, retinal pattern analysis, iris scan, voice pattern identification, and DNA analysis. The individual must be present for issuance and verification of the identifier. Issuance and verification require special equipment to scan or read the specific biometric attribute used for the identifier. Biometric identifiers are used by government agencies such as those concerned with law enforcement and immigration. The biometric information can be

stored in digitized form in electronic records and on identification cards. Biometric identifiers are not widely used as health identifiers.

Positive Aspects

- Biometric identifiers can uniquely and positively identify the patient.

Negative Aspects

- There is currently no infrastructure to issue the identifiers or maintain them nationally.
- Special equipment must be present when the identifiers are issued or verified.
- The special equipment needed would add to the cost of this option.
- The patient must be present when the identifier is issued or verified. It has been estimated that 80 percent of the times when patient records need to be accessed, the patient is not physically present; for example, when the patient telephones the provider for consultation.
- The biometric identifier would need to be digitized in order to be used for administrative simplification. Digitized images would require large amounts of storage.
- Some biometric attributes can change due to age, injury, or disease.
- Biometric identifiers such as fingerprints and deoxyribonucleic acid (DNA) profiles are commonly used in law enforcement and judicial evidence. If these kinds of identifiers were also used for health care, it might be difficult to prevent linkages that would be punitive or would compromise patient privacy.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in areas related to conciseness (the size of the digitized identifier), cost- effectiveness of producing and using the identifier for the entire population, and the equipment requirements. Some of the positive aspects of this proposal, as revealed by the ASTM criteria relative to other proposals, are that it is unique (identifying one and only one person) and atomic (not containing subelements with meaning).

3. Personal Immutable Properties

Description

Many variations of this type of identifier exist. The ANSI HISB Inventory of Standards described one particular proposal from this type. It is designed as a 19-digit number, although a method of compressing it to a 10-digit identifier by expressing it as a base 34 number was described. It would have three immutable values plus a check digit, with each separated by a delimiter. The first value is a 7-digit date of birth (using only the last three digits of year), the second is a 6-digit geographic code based on degrees of longitude and latitude, and the third is a 5-digit sequence number assigned by an area jurisdiction, with an international registry administered by an organization such as the World Health Organization. Temporary assignments would have a leading "T." In general, the proposals for identification based on personal immutable properties involve an identifier based on a combination of a person's characteristics that would not change (for example, birth name, date of birth, place of birth, gender, mother's maiden name), possibly in combination with a sequential identifier to form a health care identifier.

Positive Aspects

- Under some of the proposals, a person would not have to remember a new number, since the identifier would contain known elements.

Negative Aspects

- All of the proposals concerning Personal Immutable Properties would require the creation of a new system for assigning and maintaining the number. None included a description of a cost-effective infrastructure to administer the system.
- None of these proposals provided a method of ensuring that the person presenting the identifier was the person to whom the number was assigned.
- An individual's unique identifier possibly could be assembled by someone who knows personal details about the individual and then could be used fraudulently.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in the areas of being atomic (a single data item without meaningful subelements), being content-free, and being cost-effective. It would also be relatively difficult to use by manual systems. One of the positive aspects of this proposal as revealed by the ASTM criteria relative to other proposals was in the area of verifiable (able to determine validity of the identifier) and assignable (possible to assign whenever needed).

4. Civil Registration System

Description

This proposal would use records established in the current system of civil registration as the basis to assign a unique, unchanging 16-position randomly-generated (in base 10 or base 16) identifier for each individual. Uniqueness would be established based on data, such as name, date of birth, place of birth, and mother's first name, present in the civil records. The 16-digit unique identifier would link the lifetime records of an individual's human services and medical treatments. A system would be developed to track these and other encounters with the civil system. Tracking would occur through rank-ordered documents--first order would be state birth files, visas, "green cards," etc.; second order would be SSA records and military identification, etc.; and third order would be library card and membership in civic organizations, etc. To guard against unauthorized access of records, and to ensure the voluntary participation of the individual in the tracking and linking of his/her records, each individual would choose a personal identification number (PIN). Such a feature would operate much as does the combination of an Automated Teller Machine card and PIN in accessing bank records. This proposal has not been piloted, and no cost estimates are available.

Positive Aspects

- This proposal meets the requirement of HIPAA for a standard, unique health identifier for each individual.

Negative Aspects

- This proposal would not allow for an identifier whose use could be specifically limited to health care and appropriate related uses.
- The coordination that would be required among the State-based birth registration agencies (which do not operate in a uniform way) would be a major barrier to the implementation of this proposal.
- The cost of implementing this entirely new system would be high because of the need for a new infrastructure.
- Any system that tracks all health and human service encounters would be likely to raise very strong privacy objections.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in the areas of being focused for health care (created and maintained solely to support health care), being cost-effective, being able to be assigned retroactively, and being verifiable (able to determine validity without additional information). Some of the positive aspects of this proposal, as revealed by the ASTM criteria relative to other proposals, were in the areas of being permanent (never assigned to someone else) and public (able to be revealed).

D. Proposals That Do Not Require a Universal, Unique Identifier

1. Identification Methods Based on the Master Patient Index Concept

Several identification system proposals are based on the Master Patient Index concept. These proposals attempt to address the challenge of locating and linking medical records across organizations or enterprises, without requiring the use of a unique identifier. While individual institutions currently use Master Patient Indexes, the other proposals in this group have not been piloted, and no cost estimates are available.

- **Master Patient Index**

A Master Patient Index (MPI) is a commonly-used system in health care that links a patient medical record number with a limited set of common identification elements known to a patient, such as patient first name, patient last name, sex, birth date, SSN, and mother's maiden name. A patient seeking care provides the common elements; the MPI system matches the common data elements across its index to identify the patient's medical record number, which is required to retrieve the patient's record. Because this system is already in use successfully in many sites, some people see no need for a unique health care identifier.

Multiple sites within a large organization may keep their own separate medical records and have separate medical record numbering systems and separate MPIs. The separate MPIs may use different matching processes to obtain the medical record number. MPIs often have different identifying elements and sometimes lack any common identification number for the patient, although the SSN is frequently used as the identifier. This means that, for example, in one large health care enterprise, the hospital, the emergency services department and one or more outpatient clinics may each have separate medical record numbering systems and separate MPI systems. When organizations merge, it is very difficult to merge MPIs, since each system brings a historical data set with one or more identification numbers, possibly of various lengths, with no guarantee that there will be a common non-health care assigned number. When an enterprise attempts to integrate its systems, merging may reveal data integrity issues, including duplicate records. The merging process must not only match records that have some identical identifiers, but must identify possible matches when the records' identifying data are inconclusive. Performing the final verification usually requires human intervention.

- **Directory Service**

This proposal would use legacy system directories at local sites of patient care and cross reference directories to records at other sites. The legacy system directories would consist of patient characteristics such as name, address, SSN, race, sex, biometric identifiers, and local patient identifiers to identify the individual. The concept of the legacy system directory is similar to that of a Master Patient Index. The legacy system directory would be coupled with a system of cross reference directories to provide linkages to records of individuals across systems. The directory service would use these directories to search across patient record systems to locate prior points of care for the individual and electronically

exchange network addresses so that linkages could occur.

- Common Object Request Broker Architecture, Healthcare Domain Task Force (CORBAmed) Person Identification Service (PIDS)

CORBAmed is the health care component of the Object Management Group, an industry consortium that promotes application of Object Oriented Technologies. CORBAmed has issued a Request for Proposals for development of the CORBAmed PIDS, which is intended to facilitate communication across multiple levels of Master Patient Indices. CORBAmed PIDS would support the identification of people receiving care at a specific site and the correlation of identifiers and records of people who have received care in different sites. It would permit and support a broad range of confidentiality policies.

- Sequoia Software Award for Research and Development of a National Master Patient Index

In October 1997, the U.S. Commerce Department's National Institute of Standards and Technology awarded Sequoia Software Corporation a research and development grant to develop a Master Patient Index that can correlate and cross reference computerized patient records from different health care organizations. The goal is to match records across a national computer network without the need for human intervention.

- Health Level Seven (HL7) Master Patient Index Mediator

The HL7 mediation is a software process that searches and locates patient records across separate Master Patient Indices. HL7, an accredited standards development organization, has established a Special Interest Group to propose and develop the process by which identifying information will be located and matched.

Positive Aspects of Proposals Based on a Master Patient Index Concept

- These proposals would not require any changes to implement a unique health identifier. Existing numbering systems would continue to be used, reducing costs associated with changing over to a unique health identifier.

Negative Aspects of Proposals Based on a Master Patient Index Concept

- These proposals would not provide a unique health identifier that could be used, for example, on a health insurance claim or to label a laboratory vial.
- These proposals depend upon search, match, and link functions that have not been implemented in the health system on a national scale.
- These proposals depend upon provider organizations' participation in the processes to update directories and to link and match information.
- These proposals require development of processes that can protect individual privacy while permitting searches and matches based on personal characteristics.
- Matching depends upon the probability that records having certain data characteristics in common belong to the same individual. Human intervention is required in some cases to confirm the final match.
- Those proposals depend to some extent on new technology that has not been tested on a national scale.

Application of the ASTM criteria revealed many negative aspects of this proposal relative to others in

the areas of being focused for health care (created and maintained solely to support health care), being unique (identifying one and only one person), atomic (not containing subelements with meaning), concise, content-free, cost effective, permanent, unique, and unambiguous. These reflect the quality of not having one controllable number that can be governed for health care related uses. Some of the positive aspects of this proposal, as revealed by the ASTM criteria relative to other proposals, were in the areas of accessibility and assignability.

2. Identification Systems Based on Existing Medical Record Numbers with a Practitioner Prefix

Description

This candidate identifier proposal was listed in the ANSI HISB inventory. This proposal is for a practitioner prefix to be added to the medical record number. The most common method of identifying an individual in health organizations is through use of a medical record number. Each provider organization maintains a Master Patient Index and assigns and maintains the medical record number based on identifying information in the index. The medical record number is unique only within the provider organization. The two- position practitioner prefix would indicate a practitioner that maintains medical records on the individual. The medical record number would identify the individual's record within the practitioner's data base. The individual would designate one practitioner that would have primary responsibility for linking and updating the information in the individual's medical record. This proposal has not been piloted, and no cost estimates are available.

Positive Aspects

- This candidate would not require implementation of a unique health identifier and its related infrastructure. Existing numbering systems would continue to be used.
- A central trusted authority would not be needed.
- Implementation costs would be low.
- The addition of the practitioner prefix would minimize situations in which the same medical record number is used for different individuals within an institution.
- Some privacy fears would be addressed, since the patient would be able to control whether past medical records could be found.

Negative Aspects

- The medical record number with practitioner prefix would be unique to an individual only within an institution, for example, a hospital or a managed care organization.
- The medical record number with practitioner prefix would not be permanent; it would change when the practitioner changed.
- The medical record number with practitioner prefix would not permit the linkage of records from different institutions for valid administratively or clinically necessary applications.
- The proposal would require the practitioner designated by an individual to take on the role of updating information in the individual's medical record and linking it to the individual's other sites of care.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in the areas of being governed, identifiable, repository-based, verifiable, unique, and permanent. These aspects reflected the proposal's purpose of not facilitating linkages across systems. Some of the positive aspects of this proposal, as revealed by the ASTM criteria relative to other proposals, were in the areas of accessibility, assignability, usable, and focused.

E. Hybrid Proposals

1. The UHID/SSA Proposal

Description

This proposal consists of a unique identifier based on the properties of the Sample UHID as described in ASTM's Standard Guide, with the SSA as the trusted authority for assignment and maintenance. This proposal has not been piloted, and no cost estimates are available.

The identifier under this proposal would have the same structure as the Sample UHID, discussed above. It would consist of four parts: (a) a sequential number that identifies an individual uniquely, (b) a delimiter, (c) one or more check digits, and (d) an encryption scheme identifier to allow for extra protection of a patient's identity in sensitive situations. Unlike the ASTM Sample UHID, the UHID/SSA proposal does not specify the lengths of each of the components of this identifier. In a later section, Implementation Issues Needing Further Consideration, we solicit input on the appropriate lengths and, where applicable, algorithms for each of these components.

The UHID/SSA proposal selects the SSA to become a "trusted authority" for providing the infrastructure and maintenance of the UHID/SSA and with issuing the health identifier as part of its re-validation procedure, discussed above. This proposal echoes the call for improvements to the birth certificate process to ensure reliable issuance of SSNs and UHIDs at birth. It would also make obtaining false SSNs and UHIDs by altering, counterfeiting, or obtaining fraudulent evidence documents more difficult. As the SSA validates new applicants for SSNs to be unique, it would issue the UHID. People who do not have SSNs would be issued UHIDs as they generate their first encounter with the health system, as discussed below. The UHID would not be placed on the card used to issue the SSN. The SSA would maintain the database linking the SSN with the health identifier for its internal verification process, but other unauthorized users would be prohibited from linking the two numbers. The SSA is an experienced public program with a national identification system that includes most U.S. citizens and with the infrastructure necessary to issue and maintain the health care identifier. The relative cost to the Government of adding a unique health identifier to SSA records should not be great.

Positive Aspects

- The UHID/SSA proposal meets the requirement of HIPAA for a standard, unique health identifier for each individual.
- Designating the SSA as the responsible authority for assigning the health care identifier builds on the present infrastructure for issuing SSNs.
- The proposal builds on the improvements needed to validate SSNs in use.
- It incorporates check digit and encryption capabilities.
- It would restrict the identifier to health care uses that can be protected with legislation or regulation.

Negative Aspects

- The cost to the industry to modify its systems and add another, longer identifier would be significant.
- The re-verification component of this proposal would be very costly to implement, according to the SSA's figures. If funding for the SSA to accomplish the re-verification is not forthcoming, an important feature of this proposal would become prohibitively expensive.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in the areas of being concise and in whether it would be cost effective. This depends on whether SSA would reverify its SSNs for reasons unrelated to its proposed role as a trusted authority. Most of the remaining aspects of this proposal, as revealed by the ASTM criteria relative to other proposals, were positive.

2. Veterans Health Administration Hybrid Model

Description

This system is currently being pilot tested. It is based on an implementation by the Veterans Health Administration (VHA). The method involves the use of a master patient index system that identifies patients using VHA services based on several identifying properties, including the SSN, and the assignment of a unique identifier that is based on the ASTM Sample UHID. The VHA terms this unique identifier an Integration Control Number (ICN). When a person who does not yet have an ICN presents for care, access is established to the centralized MPI. The central system assigns a temporary ICN. If the person is later adequately identified and is determined to already have an ICN, the temporarily assigned ICN becomes an alias to the principal ICN, and the system using the alias ICN is electronically informed to begin using the principal ICN and recording the temporarily assigned ICN as an alias.

Positive Aspects

- Use of the ICN corrects for deficiencies in use of the SSN as an identifier. The SSN serves as one item in the identification index, but is not the sole identifier.
- The ICN is used only for health care. Linkages for other purposes that might compromise patient privacy could be prohibited by legislation or regulation.

Negative Aspects

- Some of the negatives of the UHID/SSA proposal, such as length and cost to implement, carry over to this system due to their similarities.
- While this system would provide a method for records to be readily linked to other systems' records through proper channels, it would not be cost effective to implement on a national scale if an entirely new agency had to be created to provide governance.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in the areas of the ICN lacking conciseness and its cost effectiveness if extended to become a national system. Most of the other aspects of this proposal, as revealed by the ASTM criteria relative to other proposals, were positive.

F. Cryptography Methods That Are Not Identifiers

Description

The National Research Council defines cryptography as the art of keeping data secret, primarily through the use of mathematical or logical functions that transform intelligible data into seemingly unintelligible data and back again. As noted earlier, cryptography is not actually an identifier, but a means to protect identifiers through the application of encryption technology. The ANSI HISB Inventory of Standards described this method as a two-key system that would allow data to be encoded with one key and decoded with another key in such a way as to reveal the patient identity only to entities with both keys, one of which would be in the control of the patient.

The United States Postal Service is developing new electronic commerce services that include methods to ensure the security and privacy of electronic information. The Postal Service cryptography and public key management services might be useful components of public/private key management for a health identifier. These services, however, have not received robust testing for implementation on a national scale, and no cost estimates are available.

Positive Aspects

- Public/private key management schemes are now proven technology and could be used as part of any unique health identifier for individuals implementation scheme that is adopted.

Negative Aspects

- The infrastructure necessary to distribute and support the keys to everyone in the population would be prohibitively expensive to implement in the 2-year time frame allowed by the law.
- The educational and cultural challenges associated with training all adults in the use and control of encryption keys would be significant.
- This scheme does not address the need to identify records when the patient is not present or is not able to provide the private key.

Application of the ASTM criteria revealed negative aspects of this proposal relative to others in the areas related to the technical nature of this proposal, particularly the characteristics of being usable (processable by both manual and automated means), verifiable, public, concise, and deployable (implementable using a variety of technologies). Some of the positive aspects of this proposal, as revealed by the ASTM criteria relative to other proposals, were in the areas of atomic (a single data item without meaningful subelements), content-free, focused, and permanent.

IV. Implementation Issues Needing Further Consideration

All of the proposals have implementation issues that would need to be resolved. We discuss and seek comment on the implementation issues below. We note that some of the issues, such as those presented in parts IV.A., B., C., and D. below, apply only to those proposals that include an identifier.

A. Temporary Identifiers

A system would be required to learn the identifier for an individual who has one but is unable to provide it, to assign a temporary identifier for an individual who has none or whose identifier is unknown, and to manage the linkage of temporary and permanent identifiers. The complexity, cost, and potential for error associated with management of temporary identifiers could be significant. We welcome feedback on ways to reduce complexity, cost, and error. We can distinguish two kinds of situations in which temporary identifiers would be necessary:

(1) Most of the candidate identifier proposals would require the individual to submit information and the trusted authority to verify the individual's identity before assignment of a permanent identifier. Under this type of process, if the individual's identity could not be quickly and positively authenticated to satisfy the requirements for a permanent identifier, the trusted authority would assign a temporary identifier that would be controlled at the national level. Under one possible scenario, temporary identifiers would have the same structure as permanent identifiers, but would be reserved from the pool of permanent identifiers. They would be unique nationwide. The temporary health identifier would be used for any episodes of care until the trusted authority could adequately verify the identity of the

individual. Once identity was verified, if the trusted authority found that this individual did not already have an entry in the identifier index, the "temporary" health identifier would become the permanent unique health identifier. On the other hand, if an entry were found to exist in the identifier index, the temporary identifier would be recorded as an alias identifier, which would be merged with the permanent unique health identifier. The trusted authority would inform the individual and the health care provider of the permanent unique health identifier.

(2) Temporary identifiers would also be required for emergency care of unconscious individuals, infants, or those with significant language barriers. A provider would issue a temporary identifier for an individual when the unique health identifier is unknown. Each provider would be responsible for the format of its own temporary health identifiers. The temporary health identifiers would be unique within the provider's system, but not unique nationwide. The provider would find out the permanent identifier from the patient at a later time. When this is not possible, the provider would transfer the individual's identifying information to the trusted authority, and the trusted authority would determine if a permanent unique identifier had already been issued to the individual. If not, it would assign a temporary health identifier or assign a permanent one and would inform the individual and the health care provider of the permanent unique identifier. The provider would then change the patient number of record, replacing the temporary identifier that the provider produced with the temporary health identifier or the permanent one of the trusted authority.

B. Encryption of the Identifier

A method of encrypting the unique individual identifier would be required for circumstances in which the identity of the individual needs to be obscured. The encryption of the identifier to obscure the identity of the individual is distinguished from encryption of entire medical records or messages in transmission. The Standard Guide indicates it would be desirable to be able to generate an arbitrary number of encrypted identifiers from any primary identifier. An encrypted identifier would be used during a single patient care episode, for example, reporting a sensitive laboratory test. The encryption scheme used to generate the encrypted identifier could be designated by an encryption scheme identifier, which could be appended to the encrypted identifier or could be stored separately. The algorithms and keys used to encrypt and decrypt would be known and used only by the trusted authority. Encrypted identifiers would be treated as aliases to the identifier. Capability for encryption of the identifier could add to its length. The encryption requirements would also add to the complexity and cost of the infrastructure that would link the original and encrypted identifiers and manage the encryption and decryption schemes. We are specifically soliciting public comment on to what degree is encryption of the identifier an essential part of an acceptable identifier design? Under what conditions is encryption of the identifier appropriate? What are the costs and benefits of identifier encryption?

C. Length of the Identifier

The optimal length of the identifier should be considered. A longer identifier would increase storage and transmission costs and would decrease ease and accuracy of manual use. We do not know how great these impacts would be.

Some people believe that an identifier format that is longer than that of the identifiers in common use would pose significant conversion burdens. Replacement of current identifiers in existing record formats with a new, longer identifier would require health plans and providers to modify their information systems and record formats.

Other people believe that health plans and providers will choose to add a new identifier to existing

record formats rather than replace existing identifiers. In this case, record formats would need to be modified, regardless of the length of the new identifier, so the length of the new identifier would not significantly affect conversion costs.

We invite the public to comment on what is the optimal length of the identifier and why?

D. Check Digits

The selection of a recognized International Standards Organization check digit or multiple check digits should be evaluated for use with any identifier being considered. Multiple check digits add length to the identifier but are able to detect more kinds of errors than a single check digit. Check digit algorithms are usually designed to be calculated from all-numeric base numbers, but the inclusion of alphabetic characters may be a desirable design for an identifier because it would increase the capacity of a shorter identifier. However, any alphabetic characters in the identifier would need to be translated to specific numbers before the calculation of the check digit, and this conversion would diminish the effectiveness of the check digit in detecting errors. Some people believe that a check digit is a critical part of the identifier design because it can help detect keying errors. Other people believe that the identifier will not need to be keyed in the majority of its uses, since it will already be in a record or on a card. These people believe that the check digit has been overvalued.

The length of the identifier and the error detection capabilities of the check digit must be balanced in selecting the optimal identifier and check digit design. It is critical to recognize that the cost and benefits of check digits could vary significantly depending on the type of identifier selected. For example, the cost to include a check digit in a completely new identifier is minor since most systems will have to be changed anyway to accommodate the new number. On the other hand, the cost of adding a check digit to the SSN would be very significant because the current systems that use the SSN would not have to change otherwise. In addition, other authenticating data can mitigate the need for a check digit. Some people believe that if an online, real-time name and number verification capability were available to anyone who would need to record or verify the identifier, a check digit would provide little additional value.

We solicit public comment specifically on to what degree are check digit(s) a desirable part of the identifier design? What specific check digit scheme is preferred, if any? What are the costs and benefits of using check digit(s)?

E. Compatibility with Evolving Technologies

Any identifier selected should be independent of particular information technologies and flexible enough to adapt to new ones. Do the candidate identifiers meet the requirement for flexibility with respect to future scenarios of record keeping and data transmission?

F. System Infrastructure, Availability, and Access

The identifier system would assign identifiers, match patient information, and verify the unique health identifier for individuals. It would also manage temporary health identifiers, encrypted health identifiers, and linkages among alias health identifiers. We solicit comment on what kind of computer and communications infrastructure is required to support an individual identifier system? Does the computer network to support these functions need to provide nationwide access 24 hours a day, 365 days a year? What kinds of entities should have access to the system and for what purposes?

G. Assignment of Unique Health Identifiers for Individuals

Policies and procedures will have to be established for the assignment of unique health identifiers for individuals. The following are some of the questions that will need to be answered:

- Who should operate the individual identifier system?
- Who will determine whether a request for a unique identifier for an individual is authentic? Authentication could be performed by providers, health plans, the trusted authority or some combination of these entities.
- What kind of authentication should be required to obtain a unique health identifier for individuals? How will the system of authenticating requests and assigning unique identifiers for individuals work on a day-to-day basis? Should a birth certificate or passport be required for authentication? Should an SSN or driver's license be required?

Some people believe that for a new identifier to have value over existing identifiers, it must be established on stringent authentication and verification standards. Other people believe that authentication and verification requirements for a health identifier should not be as stringent as, for example, those required to obtain an SSN. These people believe that assignment of more than one health identifier to a single individual would rarely have severe consequences and that there would be little incentive for fraudulent assignment of health identifiers. They believe that the cost of authentication and verification outweighs the benefits of accurate, unique identification. The desired degree of authentication will be determined by balancing accuracy of identification with cost of verification. What is the appropriate standard to apply to these questions?

- Who can request a unique health identifier? Under what circumstances may someone request an identifier on another's behalf?
- How will individual health identifiers be assigned to the existing population?
- Do incidents of mistaken assignment of duplicate identifiers to an individual need to be distinguished from incidents of fraudulent acquisition of duplicate identifiers? How?

H. Implementation and Transition

Each provider and health plan will need to develop an implementation plan and transition process for using the new individual identifier. Many providers and health plans will add the new individual identifier to existing records and tables rather than replace existing individual identifiers. The new identifier is required by HIPAA to be used in certain administrative electronic health transactions. It is likely that providers will use it in clinical records and internal communication, as well as in the external communications where it is required by law. The implementation plan for the new individual identifier should be designed to lessen the burden on small providers. Some providers might find it advantageous to use a third-party clearinghouse or communications agent to comply with the requirements to use the individual identifier. The communications agent would convert paper and legacy identification data into the formats required to obtain individual identifiers from the trusted authority.

How can a smooth transition to the individual identifier be accomplished? How can the burden on small entities be lessened?

I. Costs of SSN Reverification

Both the CPRI and UHID/SSA proposals specify that comprehensive reverification of the SSN is a critical element of successful implementation. The cost of this reverification has been estimated by SSA

at several billion dollars; however, no funds have been appropriated for the task. This raises some critical questions:

- If the SSN reverification were to be carried out, what strategies would be appropriate for funding the reverification, e.g., Congressional appropriations, user fees, etc?
- How dependent is the success of the UHID/SSA and CPRI proposals on the SSN reverification being carried out in a timely fashion?

J. Costs to Implement a New Identifier for Individuals

We have no reliable estimates of costs or benefits available for any of the proposed individual identifiers, other than those associated with the SSN reverification. There are a wide range of areas where costs may be incurred. Costs may be incurred by individuals, providers, employers, health plans, state governments, and the Federal Government. Cost would include, for example, the conversion of existing systems, conversion of forms and cards, storage of a check digit, inclusion of a check digit in records/forms/cards where a human would see the identifier, and inclusion of alpha characters in the identifier. What will it cost to transition to the individual identifier system and to operate it? Who should pay those costs and why? How can costs be mitigated, particularly those costs that can be determined not to be recoverable through the improved efficiencies of a unique individual identifier?

The importance of finding a cost effective means to issue a unique individual identifier for health care cannot be overstated. We welcome comments from individuals or organizations with information about the costs of implementing the various proposals. In an attempt to gather more specific information from industry as to the expected costs of implementation for specific characteristics of a unique individual identifier, members of the Workgroup for Electronic Data Interchange (WEDI), a health industry consortium, were asked for informal feedback. Questions were posed relating to the cost of an increase in length of the identifier from 9 to 16 digits, cost to add a check digit, the change from numeric to alphanumeric, and changes to the systems that would result from making the new identifier the “working index key,” not just an additional field.

A number of WEDI member organizations responded, but only five of the responses contained specific cost estimates for implementation by an organization. They ranged from a low of \$10 thousand to a high of \$370 million. The \$10 thousand response was for one hypothetical organization to change the length of the identifier from 9 to 16 digits. The change would involve field and screen changes and the conversion of existing data. This respondent also said that if a check digit were added the additional cost would be \$5 thousand, but the resulting increased accuracy would offset this cost. A State Medicaid program responded that its cost would be \$5.7 million to expand to 16 digits and change to an alphanumeric field type, assuming the new identifier became the working index key. A large insurer responded that such a change to its statewide system would be a massive undertaking, costing about \$370 million. The cost would drop to \$7.2 million if they could still use the SSN for internal identification purposes. The insurer expressed concern about having to undertake this kind of conversion while still trying to address the date problem associated with the century change.

Adding a check digit did not appear to raise concerns with any of those responding. Several responded that a new patient identifier would probably be added as a new, alternate key rather than replace the current primary index key and all of its logic. Responses indicated that expanding the field length from 9 to 16 digits would be a major database conversion for their system, but one questioned why it would need to be longer than 12 digits. Several said they currently allow up to 12 digits. There was lack of agreement on whether the identifier field should be numeric or alphanumeric. The responses indicated that increasing the length of a field increases the cost, and that alphanumeric fields of the same length are more costly than numeric. However, an alphanumeric structure might be less costly if it resulted in a

shorter field length. Two responses suggested that in the name of simplification we should just adopt the least expensive alternative, the SSN. The responses reflect the absence of a consensus within the industry as to which standard to adopt for this identifier.

Are these concerns valid? How? What are some alternatives?

K. Time Frames for Implementation

HIPAA mandates that implementation of each identifier be completed within 24 months after adoption of the final rule for that identifier. In the case of the identifier for individuals, what strategies will help the various potential users of the identifier (for example, individuals, providers, employers, health plans) be ready by this date?

L. Relationship of Other HIPAA Standards to Identifier for Individuals

It is likely that standards for the electronic transactions required by HIPAA will be adopted before the standard for the unique identifier for individuals. What are the implications of implementing the transaction standards without a standard identifier for individuals? Should the implementation time frame for the identifier for individuals be related to the passage of privacy legislation?

7/2/98