Designation: E 1714 – 00

An American National Standard

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

This standard is issued under the fixed designation E 1714; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide covers a set of requirements outlining the properties of a national system creating a universal health care identifier (UHID). Use of the UHID is expected to be limited to the population of the United States.

1.2 This guide sets forth the fundamental considerations for a UHID that can support at least four basic functions effectively:

1.2.1 Positive identification of patients when clinical care is rendered;

1.2.2 Automated linkage of various computer-based records on the same patient for the creation of lifelong electronic health care files;

1.2.3 Provision of a mechanism to support data security for the protection of privileged clinical information; and

1.2.4 The use of technology for patient records handling to keep health care operating costs at a minimum.

1.3 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 *ASTM Standards:*

E 1384 Guide for Description for Content and Structure of an Automated Primary Record of Care[2]

3. Terminology

3.1 *Definitions:*

3.1.1 *clinical record linkage*—individual unit records linked for the purpose of documenting the sequence of events or care, or both, for a specific patient.

3.1.2 *discriminating power of an identifier*— the capability of an identifier to reduce the possible global population to a smaller number. For example, sex identification reduces the population size to approximately half. Date of birth reduces the population size to approximately one of 25 000 in the United States. The smaller the population size covered by an identifier (that is, the greater the discriminating power), the better that identifier is.

3.1.3 *encounter*—an instance of direct (face-to-face) interaction, regardless of the setting, between a patient and a practitioner vested with primary and autonomous responsibility for diagnosing, evaluating, or treating, or some combination thereof, the patient's condition or providing social worker services. (Encounters do not include ancillary services, visits, or telephone contacts) (see Guide E 1384).

3.1.4 *encrypted universal health care identifier (EUHID)*—a UHID that has been encoded in order to disidentify the person associated with that UHID.

3.1.5 *episode of care*—a chain of events over a period of time during which clinical care is provided for an illness or a clinical problem (see Guide E 1384).

3.1.6 *healthcare identifier*—a tag for the identification of an individual created for exclusive use of the health care system.

3.1.7 *identifier*—a datum, or a group of data, that allows positive recognition of a particular individual.

3.1.8 *occasion of service*—a specified identifiable instance of an act of service involved in the care of patients or consumers (see Guide E 1384).

3.1.9 *permanent identifier*—a characteristic feature of an individual that generally does not change over time, such as sex, date of birth, place of birth, or fingerprint.

3.1.10 *prospective record linkage*—successive documentation of clinical encounters so that all records are linked during the process of care to ensure the continuity of patient care. Linkage is performed at the unit record level and occurs during the time the patient is receiving care. For electronic health records, prospective record linkage involves linking all patient assessment, diagnostic, treatment, and other information collected by all care providers so that the information is available at the time the patient is being treated. All records for an individual patient will be linked accurately since errors will be discovered and corrected in the process of providing care.

3.1.11 *retrospective record linkage*—matching unit records in data files not originally designed to be linked. The purpose of the linkage is to expand the comprehensiveness of each file being linked to facilitate evaluations of efficiency and effectiveness. Linkage can be performed manually using the actual paper records if the files are small. Linkage is more efficient if

[1] This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.25 on Healthcare Management, Security, Confidentiality, and Privacy.

Current edition approved Oct. 10, 2000. Published November 2000. Originally published as E 1714–95. Last previous edition E 1714–95.

[2] *Annual Book of ASTM Standards*, Vol 14.01.

performed probabilistically using computerized data if the files are large and conditions of uncertainty exist concerning what should be linked. (H. B. Newcombe was the pioneer developer of retrospective probabilistic record linkage.[3]) Not part of the process of patient care, this linkage occurs some time after the patient has been discharged and after the records have been computerized and merged into data files that may be managed at the facility, regional, or state level. Not all records that should link are expected to link because of missing or inaccurate data and missing records. Typical data files linked retrospectively include birth and death certificates, disease registries with hospital discharge records, emergency medical services (EMS) crash records, and hospital discharge records statewide.

3.1.12 *temporary patient identifier*—a unique identifier created by an institution to serve as an interim identifier when an individual's UHID is not available. All information is to be transferred to the UHID when the UHID becomes available.

3.1.13 *universal healthcare identifier (UHID)*—a healthcare identification system designed so that a healthcare identifier can be assigned to every individual.

3.1.14 *universal healthcare identifier computer system*—an automated system that can perform the functions needed to support a UHID, for example, verifying the validity of a UHID.

3.1.15 *universal healthcare identifier system*—the agencies, system, and networks that implement a UHID and conduct associated activities.

3.1.16 *universal healthcare identifier trusted authority*—a computer system and its associated organization that is able and authorized to provide UHID services, such as granting new UHIDs and supporting UHID encryption and decryption services.

3.1.17 *variable identifier*—those personal characteristics that may change over time such as home address, telephone number, insurance number, or name.

3.1.18 *visit*—the visit of an outpatient to one or more units or facilities located in or directed by the entity maintaining the outpatient health services (such as a clinic, physician's office, hospital, or medical center) (see Guide E 1384). Visits provide a count of the number of patients seen. It is possible for a single patient to have more than one encounter and more than one occasion of service during a visit.

4. Significance and Use

4.1 Recent explorations of the feasibility of computer-based patient records (CPRs) have revealed many valuable potential benefits, but it has also become apparent that the effective application of high technology will create some new problems. CPRs offer the option for lifelong linkage of all records on a patient, from birth to death. Such longitudinal record linkage would make the patient's entire past health history retrievable. This could make possible a quantum leap in the clinical practice of health care, but a reliable patient identifier is essential to make such a large-scale nationwide record linkage feasible. The design of a patient identifier system is not a simple task. Incorrect record linkage would create confusion, at least, or possibly cause serious consequences. To gain the benefits from such an identifier, it must be used by all relevant organizations. A national patient identifier system must resist unauthorized access to confidential clinical data. Furthermore, the creation of personal identifiers for the entire population must be a cost-effective process in light of the current fiscal constraints. The creation and administration of personal identifiers for the entire population must be accomplished at a cost that is widely accepted as affordable and justified. Last, but not least, a time pressure exists. The solution to the patient identifier challenge should use technology to facilitate rapid deployment throughout the United States to permit the expeditious implementation of CPRs.

5. Different Types of Computer-Based Patient Records

Clinical Event	Documentation
(1) Single encounter (such as office visit)	Record of a single visit
(2) Single episode of care (such as a hospitalization)	Records of a series of consecutive clinical activities
(3) Multiple encounters at same site, linked (such as clinic or longitudinal office records)	String of discrete records
(4) Multiple episodes, same institution (for example, multiple admissions)	String of discrete groups of records linked by hospital number
(5) Multiple encounters or episodes, at different sites	Unlinked, to be linked in order to form longitudinal health care file
(6) Perinatal records	To include parents' health history, pregnancy, birth, and puerperal and neonatal records
(7) Death records	Final illness record, to be linked to next generation's family history, closing, and summary record

6. Criteria and Characteristics of a Universal Health Care Identifier

6.1 The UHID should meet *at least* the following criteria (listed in alphabetical order):

6.1.1 *Accessible*—New UHIDs should be available whenever and wherever they are required for assignment.

6.1.2 *Assignable*—It should be possible to assign a UHID to an individual whenever it is needed. Assignment will be performed by a UHID trusted authority after receiving a properly authenticated request for a new UHID.

6.1.3 *Atomic*—A UHID should be a single data item. It should not contain subelements that have meaning outside the context of the entire UHID. Nor should the UHID consist of multiple items that must be taken together to constitute an identifier.

6.1.4 *Concise*—The UHID should be as short as possible to minimize errors, the time required for use, and the storage needed.

6.1.5 *Content-Free*—The UHID should not depend on possibly changing or possibly unknown information pertaining to the person.[4]

6.1.6 *Controllable*—The confidentiality of EUHIDs can be ensured. Only trusted authorities have access to encryption and

[3] Newcombe, H. B., *Handbook of Record Linkage*, Oxford University Press, Oxford, England, 1988.

[4] Including content in the UHID makes it impossible to assign the "correct" identifier if that information is not known. It also leads to invalid situations if the information changes; for example, what happens to an identifier based on gender if the person has a sex change procedure?

decryption algorithms and methods and to the linkages between EUHIDs and UHIDs.

6.1.7 *Cost-Effective*—The UHID system chosen should achieve maximum functionality while minimizing the investment required to create and maintain it.

6.1.8 *Deployable*—The UHID should be implementable using a variety of technologies, including magnetic cards, bar code readers, optical cards, smart cards, audio, voice, computer data files, and paper.

6.1.9 *Disidentifiable*—It should be possible to create an arbitrary number of UHIDs that can be used to link health information concerning specific individuals but that cannot be used to identify the associated individual. These are encrypted universal healthcare identifiers (EUHIDs). With the exception of disidentification, EUHIDs should have all of the properties attributable to UHIDs, including verification (see 6.1.31). It should be clear to all users whether a specific identifier represents a UHID or an EUHID. The EUHID scheme should be capable of generating a large number (at least hundreds) of EUHIDs for a single individual. (See Section 8.)

6.1.10 *Focused*—The UHID should be created and maintained solely for the purpose of supporting health care. Its form, usage, and policies should not be influenced by the needs or requirements of other activities.

6.1.11 *Governed*—An entity shall exist that is responsible for overseeing the UHID system. This agency will determine the policies that govern the UHID system, manage the trusted authority(ies), and take such actions as are necessary to ensure that the UHIDs (and EUHIDs) can be used properly and effectively to support health care.

6.1.12 *Identifiable*—It shall be possible to identify the person associated with a valid UHID. Identifying information may include such standard items as name, birthdate, sex, address, mother's maiden name, etc. This information is not incorporated in the UHID but is associated with it by linkages.

6.1.13 *Incremental*—The UHID system should be capable of being implemented in a phased-in manner. This may include incremental implementation for a specific institution (some types of information linked using UHIDs and some using other identifiers), for the information on a specific patient, and for a geographic area.

6.1.14 *Linkable*—It shall be possible to use the UHID, or EUHID, to link various health records together in both automated and manual systems.

6.1.15 *Longevity*—A UHID system should be designed to function for the foreseeable future. It should not contain known limitations that will force the system to be restructured or revised radically.

6.1.16 *Mappable*—During the incremental implementation of a UHID, it shall be possible to create bidirectional linkages between a UHID and existing identifiers used currently by a variety of health care institutions.

6.1.17 *Mergeable*—In the (theoretically infrequent) case that duplicate UHIDs are issued to a single individual, it shall be possible to merge the two UHIDs to indicate that they both apply to the same individual.

6.1.18 *Networked*—The UHID should be supported by a network that makes UHID services universally available where needed.

6.1.19 *Permanent*—Once assigned, a UHID should remain with that individual. It should never be reassigned to another person, even after the individual's death.

6.1.20 *Public*—The UHID (but not necessarily EUHID) is meant to be an open data item. The individual it identifies should be able to reveal it to any person or organization.

6.1.21 *Repository-Based*—A secure, permanent repository shall exist in support of the UHID. The repository should contain UHIDs, patient identification data, EUHIDs, encryption and decryption methods, and other relevant information to support functions such as linkages.

6.1.22 *Retirement*—It shall be possible to retire a UHID or EUHID that is no longer active, for example, when the associated individual has expired.

6.1.23 *Retroactive*—It shall be possible to assign UHIDs to all of the currently existing individuals at the time that the UHID system is implemented.

6.1.24 *Secure*—The creation of EUHIDs, decryption of an EUHID to reveal the identity of the individual, and maintenance of encryption techniques must be performed in a secure manner to ensure that the policies governing such activities are enforced.

6.1.25 *Splittable*—In the (theoretically never occurring) event that the same UHID is assigned to two individuals, there must be a mechanism to assign a new UHID to one (or both) of these individuals.

6.1.26 *Standard*—The identifier scheme should be as compatible as possible with existing and emerging standards such as those being developed by CEN in Europe.

6.1.27 *Unambiguous*—Whether represented in automated or handwritten form, a UHID should minimize the risk of misinterpretation. (For example, the chance of confusing the number zero and the letter "O" or the number 1 and the letter "l" should be eliminated, if possible.)

6.1.28 *Unique*—A valid UHID or EUHID should identify one and only one individual. A person should have only one UHID. (Note that a person may have an arbitrary number of EUHIDs for purposes of disidentification, as defined in 3.1.4.)

6.1.29 *Universal*—A UHID system should be able to support every living person for the foreseeable future. It should be capable of expanding to encompass even larger domains, should that become desirable.

6.1.30 *Usable*—A UHID should be processable by both manual and automated means. While manual methods for such functions as verifying the validity of a UHID may require considerably more time, there should be no technical or policy inhibitions to manual operations.

6.1.31 *Verifiable*—A user should be able to determine that a candidate identifier is or is not a valid UHID without requiring additional information. This should support the ability to detect accidental misinformation, such as typographical errors. It is not meant to be able to preclude intentional misinformation.

7. Temporary Patient Identifiers

7.1 A patient will require health care under circumstances in which the UHID is not available on some occasions. Examples of such situations include the 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 that prevents effective communication. Under such circumstances, it is essential that the lack of a legitimate UHID not impede the progress of medical care. Neither should the lack of a UHID prevent appropriate linkage of the patient's information once the proper UHID has been determined. The use of a temporary patient identifier (TPI) is recommended under these circumstances.

7.2 It is assumed that situations that require the use of a TPI will be limited in time and restricted to a single institution. Each institution will be responsible for the form and use of its own TPIs but shall provide for subsequent transfer of all information from the TPI to the correct UHID once that becomes known.

8. Encrypted Identifiers

8.1 There is an acknowledged inherent contradiction between the establishment of an open UHID for purposes of identifying a unique individual and the creation of EUHIDs intended to obscure that individual's identity. An EUHID essentially creates an alias that can be used to link various information items without knowing whose information is being linked. It is generally assumed that such an alias would be used during a single patient care episode, for example, a single hospitalization or a single procedure such as ordering or reporting a sensitive laboratory test. As a result, the system shall be capable of creating multiple (hundreds or more) EUHIDs to cover potentially large numbers of care episodes for a given individual. This requirement, in turn, places a significant burden on the trusted authorities. Since they are the only entity that has knowledge of the UHID and all EUHIDs, the trusted authorities will be responsible for supporting information linkage services when EUHIDs are used, as well as providing new EUHIDs when needed. Further, since EUHIDs are being used specifically to prevent linkage with identifying information concerning an individual, a significant policy issue is the determination of when such linkage will be permitted and when it will be denied.

8.2 The emerging capability to perform public key encryption may have an impact on the requirements for a trusted authority(ies). It may be possible to devise a scheme in which each institution could create unique encrypted identifiers without requiring recourse to a trusted authority. An evaluation of the possible role of public key encryption in supporting EUHIDs would be helpful for determining whether a noncentralized encryption mechanism is feasible.

8.3 Since EUHIDs are used to provide disidentified patient information linkage, it is important that they not contain content relating to the individual. Items such as sex, birthdate, names, etc. shall be excluded from EUHIDs to prevent compromising their disidentification function.

8.4 An EUHID shall be revealable in order to serve its linkage function. It should thus be possible to print it on reports and store it in databases, etc. in a manner analogous to an individual's UHID without compromising its disidentification function.

8.5 It is possible that, through policy (for example, a court action), malfeasance, or unintended events, an EUHID may become identified publicly with the individual it disidentifies. This should not compromise future needs for disidentification. It is thus necessary to be able to issue multiple EUHIDs for the same individual. Another example of the need for multiple EUHIDs is the ordering of potentially sensitive tests such as HIV. Since the result of the test is not known at the time the test is ordered, it appears logical to use a separate EUHID to disidentify the patient for the various tests being ordered. A final example in which multiple EUHIDs may be required is the participation of a patient in multiple independent clinical trials in which blinding is required. It may be necessary to unblind one study while maintaining blinding in others.

9. Policy Decisions

9.1 The purpose of this guide is limited to the conceptual characterization of a UHID, without any involvement in implementation methodology, cost, or policy decisions. These tasks require competence, authority, and responsibility in areas different from the scientific expertise of the ASTM committee. Accomplishing this goal may involve the Department of Health and Human Services and other federal agencies, professional organizations such as the American Medical Association and American Hospital Association, etc., and the U.S. Congress, private sector, and patient community. Health care affects every member of the society. The need to provide accurate and comprehensive linkage of health information for each U.S. citizen is clear. Being able to achieve this goal in a manner that preserves privacy and confidentiality is essential. If implemented, the recommendations contained in this guide would provide the basis for substantial improvement in the health care available to the citizens of the United States.

10. Keywords

10.1 electronic healthcare records; patient identification; record exchange; universal healthcare identifier

APPENDIXES

(Nonmandatory Information)

X1. CODE OPTIONS FOR A UNIVERSAL HEALTH CARE IDENTIFIER IN THE UNITED STATES

X1.1 *Social Security Number:*[5]

X1.1.1 *Description of the Enumeration Process:*[6]

X1.1.1.1 There are approximately 1300 Social Security offices in the United States where applicants for social security numbers (SSNs) can apply for an original SSN. The applicant submits an application (Form SS-5) and evidence of age, identity, and U.S. citizenship or lawful alien status. If the applicant is not a U.S. citizen and does not have an INS document authorizing him/her to work in the United States, the applicant must also have a valid nonwork reason for needing the SSN.

X1.1.1.2 All applicants (U.S. citizens and aliens) who are age 18 or over applying for original SSNs must apply in person and be interviewed by a field office (FO) employee. Applicants for original SSNs who are under age 18, or applicants for replacement cards, can apply in person or by mail. However, aliens are advised to take their INS documents to the FO rather than mail them.

X1.1.1.3 Generally, the Social Security Administration (SSA) does not assign SSNs to individuals who are illegal aliens. However, an illegal alien will be assigned a nonwork SSN if he/she will be paid benefits payable in whole or in part from federal funds.

X1.1.1.4 Generally, SSNs are not assigned to individuals who live outside the United States unless they are U.S. citizens or residents. However, a nonresident alien who establishes an acceptable nonwork need for a SSN, for example, to be claimed as a dependent on a U.S. tax return, may be assigned a SSN. Evidence is required to support the reason for needing the SSN. Applications from those individuals outside the United States who qualify are taken by U.S. foreign service posts and forwarded to the SSA's Office of International Operations (OIO) for processing.

X1.1.1.5 SSNs are assigned centrally at the SSA's Baltimore headquarters, based on data keyed from the various FOs and OIO. Certain pieces of information concerning the SSN applicant must be obtained before an FO submits an application for an SSN for electronic processing. The essential pieces of information are as follows: applicant's full name, date and place of birth, sex, mother's maiden name, and father's name. These data elements are used to electronically screen the SSA's database for an SSN that may have been issued previously to the applicant. This electronic screening process helps to prevent the issue of more than one SSN to a number holder. If no match can be located on the SSA's files for the applicant, an original SSN is assigned by computer and a new SSN ID card mailed to the applicant. If there is a significant match on enough data elements, a replacement SSN card is issued to the number holder and the SSA's records are updated.

X1.1.1.6 A SSN is assigned within 24 h of the date the SSN application is processed into the system, assuming there were no questions concerning the data keyed into the system. Depending on the mail delivery, it usually takes 7 to 10 days for the applicant to receive the card.

X1.1.2 *Current Benefits of Using the Social Security Number as the Universal Health Care Identifier*:

X1.1.2.1 There are 1300 social security offices, in strategic positions, with well-trained personnel, detailed standard procedural guidelines, and an electronic network in place.

X1.1.2.2 The SSN could be used for patient identification upon relatively short notice.

X1.1.2.3 The SSN could serve as a UHID, but with significantly increased administrative cost.

X1.1.3 *Current Problems with the Social Security Number if Used as the Universal Health Care Identifier*:

X1.1.3.1 Enumeration at birth is incomplete and delayed. Currently, a parent can request a SSN to be assigned to his/her child at the time he/she provides information required to register the child's birth. After the state completes its birth registration process, it provides information to the SSA by tape, which is used to assign a SSN and issue a card. The SSA thus does not receive the information immediately upon the child's birth, and there is a delay between the birth of a baby and receipt of a number.

(1) Connecticut, Rhode Island, Oklahoma, Alaska, and California are not now participating in the program "Enumeration at Birth."

(2) Only 73 % of the parents in the participating states request assignment of a SSN for their children.

X1.1.3.2 The SSN is not always unique. Approximately four million individuals have more than one SSN.

X1.1.3.3 There is no exit control. The SSA does not void, destroy, delete, or rescind validly assigned SSNs, in case of death, leaving the country, etc. On March 3, 1993, 363 336 983 SSNs were on record. This represents approximately 113 million SSNs without a corresponding living person in the U.S.

X1.1.3.4 *Significant Error Level*:

(1) According to a study conducted by the Bureau of Census, 20 % of the participants did not know their own SSN;

(2) As reported by the participants, 20 % of the SSNs failed to automatically validate against the master database of the SSA, but 85 % of those failed could be resolved manually, by search of the master files;

(3) Of the study population, 3 % could not be validated at all.

X1.1.3.5 *Lack of Check Digits*—The SSN system was designed before the computer era. Therefore, no provision was made to check the errors with an effective check digit.

[5] "The Social Security Number, Policy and General Procedures," *Federal Register*, November 1922.

[6] Information provided by A. J. Young, Deputy Commissioner for Programs, Social Security Administration.

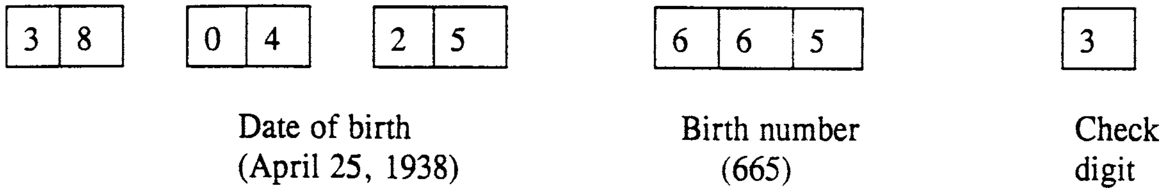

FIG. X1.1 Swedish Personal Identity Number System

X1.1.3.6 *Degree of Confidentiality*—The SSA does not disclose the SSN, or other information concerning an individual, without his/her consent unless there are reasons to disclose that are related to the administration of the social security program or other government or income maintenance programs.

X1.1.3.7 *Use of the SSN*:

(1) The Internal Revenue Service, Civil Service Commission, and Department of Defense began to mandate use of the SSN in the 1960s.

(2) States were authorized in 1976 to use the SSN to administer taxes, public assistance, driver's licenses, or motor vehicle registration.

(3) Blood donors are identified by SSN.

(4) The entire financial, banking, and commercial system, as well as the military, uses the SSN.

X1.1.3.8 *Duplicate SSNs*—A small but significant number of people have been issued duplicate SSNs.

X1.1.3.9 *Lack of Capacity*—The SSN does not have sufficient digits to handle the foreseeable future needs of health care.

X1.1.3.10 *No Disidentification Mechanism*—No scheme exists that permits SSNs to be used in a disidentified manner.

X1.1.3.11 *Expense*—SSNs are used currently in a vast number of applications by a wide variety of organizations. Making any change to these existing structures will entail substantial (perhaps prohibitive) expense.

X1.1.3.12 *Non-Public*—The SSN cannot be revealed publicly without exposing the associated individual to serious financial and privacy risks.

X1.1.3.13 *Not Controllable or Focused*—Control of the SSN is vested in organizations that are not driven by the needs of health care.

X1.1.3.14 *Cannot be Assigned as Needed*—The typical length of time required to obtain a SSN is measured in weeks rather than the minutes required by health care.

X1.1.3.15 *Not Mergeable*—No effective mechanism exists currently to merge two SSNs that have been assigned to the same individual.

X1.1.3.16 *Not Universal*—A significant number of foreign nationals, residing in this country legally and with no legitimate reason to have a SSN, will need and receive health care services here. Having no SSN, they will cause health care people to work around the system and thus introduce error.

X1.2 *Fingerprints*—Fingerprints are used by the police for criminal files. They are fully automated and claimed to be virtually error-free. The cost and social unacceptance of fingerprinting as a part of the health care process are major negative factors. An additional problem is that a fingerprint per se cannot be used for information linkage.

X1.3 *Confidential Code*—A central operation (trusted authority) could generate a random encrypted number for each person in the United States, probably via a network and multiple regional ID distributing computer centers. This five- or six-digit code would be the protective shield to prevent unauthorized access to privileged clinical information.

X1.4 *Geographic Position*—Carpenter and Chute[7] have proposed a four-component patient identifier:

(1) Date of birth	(7 digits)
(2) Latitude and longitude	(6 digits)
(3) Sequence code	(5 digits)
(4) Check digit	(1 digit)
Total:	(19 digits)

This is an imaginative design. It has the advantage of permitting the local assignment of identifiers without the risk of duplication and can be extended worldwide.

X1.5 *Swedish "Personal Identity Number"*—This identification system is mandatory. When a child is born, the parish registration office registers the birth and notifies the county tax authority. The county tax authority assigns the identity number. The design of this scheme is shown in Fig. X1.1.

X1.5.1 *Birth Number*—This is for distinguishing people born on the same day; odd numbers are used for males, even numbers for females.

X1.5.2 *Check Digit*—Using the check digit, an automated check can be made that no incorrect numbers have been entered with the date of birth or birth number.

X1.6 *Danish Personal Identifier*—The personal identifier's design is shown in Fig. X1.2.

X1.7 *Identification Scheme in Finland*—This model is shown in Fig. X1.3.

X1.7.1 *Sequence Number*—The last digit is odd for a boy and even for a girl.

X1.7.2 *Check Digit*—Divide the first nine numbers by 31. If the remainder is 1 through 9, that number is used as the check digit. If the remainder is 10, the check digit is "A," if 11, "B," if 12, "C," and so on.

X1.8 *Vehicle Identification Number*[8]—The Department of

[7] Carpenter, P., and Chute, C., *The Universal Patient Identifier: A Discussion and Proposal*, Proceedings of the 17th Annual Symposium on Computer Applications in Medical Care, 1994, pp. 49–53.

[8] Provided by V. L. Young, Jr., Criminal Justice Information Service Division, Federal Bureau of Investigation.