Designation: E1714 – 07 (Reapproved 2013)

An American National Standard

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

This standard is issued under the fixed designation E1714; 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 required to create a universal healthcare identifier (UHID) system. Use of the UHID is expected to initially be focused on the population of the United States but there is no inherent limitation on how widely these identifiers may be applied.

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:*[2]

E1384 Practice for Content and Structure of the Electronic Health Record (EHR)

E2553 Guide for Implementation of a Voluntary Universal Healthcare Identification System

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 interaction, regardless of the setting, between a patient and a practitioner vested with primary and autonomous responsibility for diagnosing, evaluating, treating, or some combination thereof, the patient's condition or providing social worker services (See Guide E1384). (Encounters do not include ancillary services, visits, or telephone contacts.)

3.1.4 *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 E1384).

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

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

3.1.7 *management organization*—an organization responsible for the management and oversight of the UHID system and its operations.

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 E1384).

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

3.1.11 *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

[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 Data Management, Security, Confidentiality, and Privacy.

Current edition approved March 1, 2013. Published March 2013. Originally approved in 1995. Last previous edition approved in 2007 as E1714 – 07. DOI: 10.1520/E1714-07R13.

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

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.

3.1.12 *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 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.) 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.

3.1.13 *temporary patient identifier*—a unique identifier used to serve as an interim identifier when an individual's UHID is not available. All information linked using the temporary patient identifier is to be transferred to the appropriate UHID when the correct UHID becomes known.

3.1.14 *trusted authority*—an organization that is able and authorized to provide UHID services, such as granting new UHIDs and supporting UHID status validation services.

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

3.1.16 *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.

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

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

3.1.19 *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 E1384). 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 experience with computer-based patient records (CPRs) has revealed many valuable potential benefits, but it has also become apparent that the effective application of this technology creates 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 large-scale regional and 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 universal 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 ongoing 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 of the system to permit the expeditious implementation of CPRs. A companion document, Guide E2553, provides the implementation strategy concerning how to actually implement the UHID system.

5. Criteria and Characteristics of a Universal Health Care Identifier

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

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

5.1.2 *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.

5.1.3 *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.

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

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

5.1.6 *Controllable*—It must be possible to ensure the confidentiality of PUHIDs. Only trusted authorities have access to algorithms and methods used to link PUHIDs and UHIDs.

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

5.1.8 *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.

5.1.9 *Disidentifiable*—It should be possible to create an arbitrary number of specialized UHIDs that can be used to link health information concerning specific individuals but that cannot be used to identify the associated individual. These are private universal healthcare identifiers (PUHIDs). With the exception of disidentification, PUHIDs should have all of the properties attributable to UHIDs, including verification (see 5.1.31). It should be clear to all users whether a specific identifier represents a UHID or a PUHID. The PUHID scheme should be capable of generating a large number (at least hundreds) of PUHIDs for a single individual (See Section 7).

5.1.10 *Focused*—The UHID system 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.

5.1.11 *Governed*—A management organization 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 PUHIDs) can be used properly and effectively to support health care.

5.1.12 *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.

5.1.13 *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.

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

5.1.15 *Longevity*—The 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.

5.1.16 *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.

5.1.17 *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.

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

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

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

5.1.21 *Repository-Based*—A secure, permanent repository shall exist in support of the UHID system. The repository should contain UHIDs, PUHIDs, and other relevant information to support the functions of the UHID system.

5.1.22 *Retirement*—It shall be possible to retire a UHID or PUHID that is no longer active, for example, when the associated individual has expired or if other circumstances (for example, fraudulent use) indicate that the identifier must be retired.

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

5.1.24 *Secure*—The creation of PUHIDs, decryption of a PUHID to reveal the identity of the individual, and maintenance of privacy techniques must be performed in a secure manner to ensure that the policies governing such activities are enforced and that patient privacy is protected.

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

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

5.1.27 *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.)

5.1.28 *Unique*—A valid UHID or PUHID should identify one and only one individual. Ideally, a person should have only one UHID. (Note that a person may have an arbitrary number of PUHIDs for purposes of disidentification. Also note that a person in rare circumstances *may* have more than one UHID. While this is not desirable, it does not represent a fatal circumstance.)

5.1.29 *Universal*—A UHID system should be able to support every living person for the foreseeable future.

5.1.30 *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.

5.1.31 *Verifiable*—A user should be able to determine that a candidate identifier is or is not a valid UHID (or PUHID) 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 or misuse of an identifier.

6. Temporary Patient Identifiers

6.1 On occasion, a patient will require health care under circumstances in which the associated UHID is not available. 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.

6.2 The UHID system shall be responsible for issuing a special class of PUHIDs that are dedicated for use as TPIs.

6.3 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 shall provide for subsequent transfer of all information from the TPI to the correct UHID once that becomes known.

7. Private Identifiers

7.1 There is an acknowledged inherent contradiction between the establishment of an open UHID for purposes of identifying a unique individual and the creation of PUHIDs intended to obscure that individual's identity. A PUHID 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 must be capable of creating multiple (hundreds or more) of PUHIDs 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 PUHIDs, the trusted authorities will be responsible for supporting information linkage services when PUHIDs are used, as well as providing new PUHIDs when needed. Further, since PUHIDs are being used specifically to prevent linkage with identifying information concerning an individual, a significant policy issue is the determination of under what circumstances such linkage will be permitted and when it will be denied.

7.2 Since PUHIDs 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 PUHIDs and PUHID-linked data sets to prevent compromising their disidentification function.

7.3 A PUHID shall be revealable (visible to any user who needs it) 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.

7.4 It is possible that, through policy (for example, a court action), malfeasance, or unintended events, a PUHID may become identified publicly with the individual it disidentifies. While unfortunate, this event should not prevent the UHID system from functioning properly if that individual has future needs for disidentification. It is thus necessary to be able to issue multiple PUHIDs for the same individual. Another example of the need for multiple PUHIDs 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 PUHID to disidentify the patient for the various tests being ordered. A final example in which multiple PUHIDs 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.

8. Blinding and Unblinding

8.1 The UHID system will create a special class of PUHID for use in situations where data needs to be blinded with the knowledge or the possibility that it may later need to be unblinded.

8.2 It will be the responsibility of the trusted authority(ies) to determine the conditions under which a PUHID may be unblinded and the process for doing so.

8.3 Note that since the blinding and unblinding requirements of each situation may differ, a unique blinded PUHID should be issued for each situation where blinding is required.

9. Policy Decisions

9.1 The purpose of this guide is limited to the conceptual characterization of a UHID and some of the characteristics of its supporting system, 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 these additional assessments may involve numerous agencies external to ASTM. Health care affects every member of society. The need to provide accurate and comprehensive linkage of health information for each person 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 everyone.

10. Keywords

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

APPENDIX

(Nonmandatory Information)

X1. SAMPLE UNIVERSAL HEALTHCARE IDENTIFIER IMPLEMENTATION

X1.1 For purposes of illustrating the use of this guide, this appendix illustrates a sample implementation of a UHID. The sample UHID is provided for the purpose of illustrating application of the various criteria listed in this standard. It is not within the scope of this guide to conduct actual evaluations of various possible UHID candidates.

X1.2 *Description of Sample UHID* —The sample UHID consists of four sub-components as diagrammed in Fig. X1.1. It consists entirely of numeric digits, except for the delimiter. The functions of each of the four components are described in X1.2.1-X1.2.4.

X1.2.1 *Prefix*—This is a 16-digit number that helps create a unique identifier. It can be assigned only by a universal healthcare identifier organization that has received a properly authenticated request for a new UHID. The new UHID is generated by a central system and assigned to the individual indicated in the request. It is permissible to create a compact representation for display purposes only of the identifier by suppressing the leading zeros in the prefix as well as the trailing zeros in the privacy class. (Note that trailing zeros in the check digits cannot be suppressed.)

X1.2.2 *Delimiter*—This is a single character that denotes the boundary between the prefix and the check digits. It is normally represented by the character "." (period), but it may also be represented by "*" when entering an identifier via a touch-tone telephone or by other mutually agreed upon delimiters when dealing with technologies that do not have "." in their character set.

X1.2.3 *Check Digits*—These eight digits are used to ensure that the identifier is valid. The check digits are computed according to an independent coding scheme by the organization that issues identifiers. They exist to ensure that incorrect identifiers resulting from typographical errors, transposition of characters, misreading of digits, data transmission errors, etc. can be detected readily. They also ensure that a false identifier created using a random string of digits can be detected readily as an invalid identifier. Note that the algorithms, keys, etc. used to create check digits are assumed to be privileged knowledge and are not in the public domain.

X1.2.4 *Privacy class*—These seven digits are used to specify a specific usage class for a PUHID. A value of 0000000 for the privacy digits indicates that the identifier is a UHID. A non-zero value for any of these digits indicates that the identifier is a PUHID. Since there are many possible circumstances in which a PUHID might be needed (for example, the participation of an individual in multiple independent clinical trials in which the blinding of patient data is required), the UHID scheme contains a sufficient number of privacy digits to support a large variety of PUHIDs.

X1.3 *Examples of Use of UHIDs and PUHIDs*—This section describes some typical uses of the UHID and PUHID to illustrate how the various components function. These examples are presented only to provide typical uses and do not necessarily correspond to any actual situation.

X1.3.1 *Assign a New UHID*—Upon receiving a properly authenticated request for a new UHID the next unique prefix is created. Seven zeros are appended to the check digits as privacy digits indicating that this is not a private UHID. The authority would then compute the proper check digits. It would then store the UHID in its database and link it with the associated patient-identifying information provided as part of the request for the UHID. The UHID would finally be returned to the party that generated the request.

X1.3.2 *Generate a PUHID*—Upon receiving a properly authenticated request for a PUHID, the organization would determine the appropriate privacy class to fulfill this request. This will determine the privacy class digits in the identifier. The PHUID prefix in the individual's UHID would then be generated. Finally, the prefix and the privacy class digits would be used to compute the proper check digits.

X1.3.3 *Decrypt a PUHID*—When a trusted authority receives a duly authenticated request to identify the individual

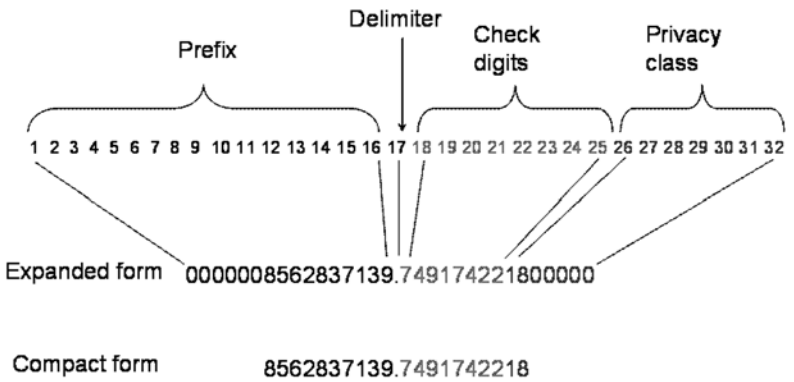

FIG. X1.1 The Anatomy of a UHID Identifier

associated with a PUHID, it does so by returning the UHID corresponding to the individual determined by the PUHID. This operation is only permitted under the conditions established for that particular PUHID privacy class.

X1.3.4 *Privacy*—The details of the algorithms and methods to create and manage PUHIDs are owned by the trusted authorities and will not be discussed here. The prefix is generated and then the proper check digits are then computed for the new PUHID in the same manner as for a standard UHID. It is assumed that the UHID organization will use a variety of encryption methods, keys, etc. The method used to create a specific PUHID for a specific patient will be specified in the privacy class digits of that PUHID. The fact that one or more of these privacy digits is non-zero will indicate unambiguously that the identifier is a PUHID rather than a UHID. Finally, note that the check digits are computed once the privacy class digits have been specified and the PUHID prefix has been created. Hence, a user can still use the check digits to verify the validity of a PUHID even though the identity of the individual linked to the PUHID is not known.