Designation: E2553 – 07 (Reapproved 2013)

An American National Standard

Standard Guide for Implementation of a Voluntary Universal Healthcare Identification System[1]

This standard is issued under the fixed designation E2553; 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 document describes the implementation principles needed to create a Voluntary Universal Healthcare Identification (VUHID) system. The purpose of this system is to enable unambiguous identification of individuals in order to facilitate the delivery of healthcare.

1.2 The VUHID system should be dedicated exclusively to the needs and functions of healthcare.

1.3 The VUHID system is designed to represent no, or at least minimal, increased risk to healthcare privacy and security.

1.4 The system should be as cost-effective as possible.

1.5 The system must be created and maintained in a way to provide sustained benefit to healthcare.

1.6 The system should be designed and implemented in a manner that ensures that it can operate indefinitely.

1.7 *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]

E1714 Guide for Properties of a Universal Healthcare Identifier (UHID)

2.2 *Other Standard:*

AIIM Standard PDF417 Bar-coding

3. Terminology

3.1 *Acronyms:*

3.1.1 *2D*—two dimensional

3.1.2 *CDO*—care delivery organization

3.1.3 *EMPI*—enterprise master patient index

3.1.4 *MO*—managing organization

3.1.5 *OVID*—open voluntary healthcare identifier

3.1.6 *PVID*—private voluntary healthcare identifier

3.1.7 *VUHID*—voluntary universal healthcare identification

4. Summary of Guide

4.1 The VUHID facility described in this guide is responsible for issuing unique personal healthcare identifiers to any cooperating EMPI facility (defined below) upon receipt of an authenticated request. The issued identifiers must be consistent with Guide E1714 and, as appropriate, would consist of both 'open' OVIDs (Open Voluntary Healthcare Identifiers) as well as PVIDs (Private Voluntary Healthcare Identifiers). This document will refer to any identifier issued by the VUHID, whether OVID or PVID, as a VUHID identifier. OVIDs are used to provide linkage of healthcare information for circumstances where the identity of the associated person is meant to be freely accessible. PVIDs (which exist in various privacy classes) permit linkage of various healthcare data items where the identity of the associated individual is *not* meant to be publicly available.

4.2 The VUHID system should be created as a secure high-availability server on the Internet which communicates exclusively with cooperating EMPI facilities using secure communication techniques. The VUHID facility issues identifiers and is responsible for maintaining policies and procedures relating to various classes of PVIDs. It does *not* store patient identification, demographic information, or clinical information and for this reason does not represent a security or privacy vulnerability. (See Section 12 for a description of how this approach is implemented when issuing a new identifier.) The VUHID facility should receive requests for information relating to a given identifier and distribute those requests to all cooperating EMPI facilities in order to fulfill the information sharing goals associated with unambiguous patient identification.

4.3 The identifiers issued by the VUHID facility can be used, consistent with the policy established for each identifier class, by all of the participating healthcare facilities interacting

[1] This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.35 on Healthcare Data Analysis.

Current edition approved March 1, 2013. Published March 2013. Originally approved in 2007. Last previous edition approved in 2007 as E2553–07. DOI: 10.1520/E2553-07R13.

[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.

with a cooperating EMPI to facilitate storage, linkage, and exchange within that system.

4.4 The VUHID facility should be controlled by a managing organization that is dedicated exclusively to the benefit of the healthcare industry.

5. Significance and Use

5.1 This standard describes a proposal to provide unambiguous personal identification for any patient who requests it. In today's world of specialized healthcare and mobile patients it is typical for clinical information on a single patient to reside in a variety of locations, some using manual data storage techniques, but an increasing number using electronic means. In order for a clinician to provide safe and appropriate clinical care in this environment it is necessary to be able to aggregate appropriate clinical information on a specific patient in order to gain an accurate and comprehensive picture of that patient's clinical situation. This implies that all information relating to each patient should be identified in a unique manner to facilitate the process of accurately aggregating appropriate information.

5.2 The converse of the need for data aggregation is the patient's need to protect the privacy of their information. Unless patients are confident that they can avoid inappropriate sharing of clinical information they will not readily share that information with caregivers. Thus, the same system that supports unambiguous linkage of all information concerning a patient must also play a role in protecting the privacy of that information.

5.3 The proposed patient identification system must be able to avoid or overcome the numerous objections that have prevented implementation of a universal patient identification system in the past including issues related to:

5.3.1 *Technology*—The proposed system must be technically feasible in a manner that promotes scalability, availability, and ease of implementation.

5.3.2 *Integration with Existing Systems*—To the maximum extent possible the proposed identification system should work seamlessly with existing information systems.

5.3.3 *Cost-effectiveness*—The proposed system should balance the costs and benefits required to implement a fully functional voluntary universal healthcare identification system.

5.3.4 *Political Feasibility*—Because many different constituencies have a vested interest in a universal patient identification system, it has been a significant challenge to gain consensus on how to implement such a system.

5.3.5 *Gradually Implementable*—In order to minimize the impact associated with its implementation, a desirable property of a voluntary universal healthcare identification system is that it be gradually implementable over time.

5.3.6 *Acceptable to the General Public*—A voluntary universal healthcare identification system must be accepted by the general public as a beneficial, effective and non-threatening capability.

5.4 Experience has shown that a healthcare identification system will only be feasible if it is dedicated exclusively to the needs of healthcare. It is only in this focused environment that it has been possible to create a consistent, feasible, functional, and effective design for such a system.

6. Anticipated VUHID Benefits

6.1 A universal healthcare identification system that is not used will offer no benefit. Since the VUHID is designed as a voluntary system, this is a significant risk if the system is not perceived by its potential users as offering sufficient value. Here is a partial list of the benefits that should accrue to people who choose to participate in the VUHID system.

6.2 *Increased Convenience*—Giving your VUHID card to a provider organization should eliminate the need to repeatedly provide a list of identifying demographic information. Instead, this information will be pulled automatically from the cooperating EMPI system.

6.3 *Improved Data Sharing*—Use of VUHID identifiers will enable clinical information to be more readily shared both within organizations and between organizations. In addition, the existence of private identifiers will enable more granular data sharing based on a variety of policy- and patient-specified principles.

6.3.1 *Locally*—The use of a VUHID should permit convenient and error-free linkage of information across all of the provider facilities operating within the domain of a cooperating EMPI facility.

6.3.2 *Nationally*—The use of VUHID should permit rapid, virtually error-free and comprehensive retrieval of any information stored within any cooperating EMPI that is participating in the VUHID network.

6.4 *Decreased Incidence of Medical Errors*—The use of VUHID identifiers permits comprehensive and virtually error-free linkage of medical records stored across a wide and heterogeneous mixture of healthcare provider facilities. Making this information available to a physician can greatly decrease the risk of inadvertent medical errors.

6.5 *Decreased Risk of Identity Theft*—Use of a VUHID identifier, particularly use of a PVID, means that an identifier, not the patient's identity, is at risk should the information be misused by a recipient or otherwise mishandled.

6.6 *Improved Control of Healthcare Information Privacy*—The ability to use various classes of PVIDs to link clinical information means that a person participating in the VUHID system has the ability to exercise precise control over various types of medical information.

6.7 *Improved Support for Clinical Trials*—Patients that participate in clinical trials can use a separate PVID to ensure that the clinical information needed for the trial is not linked to the remainder of their medical record.

7. Functions Supported by the VUHID System

7.1 Recruit cooperating EMPI facilities.

7.2 Validate each cooperating EMPI facility as a proper site to support VUHID activities and establish a contract with each cooperating EMPI site.[3]

7.3 Establish secure encrypted trusted communication with each cooperating EMPI facility.

7.4 Issue unique identifiers upon request from a validated cooperating EMPI facility and for each issued identifier log the time/date and the identity of the cooperating EMPI facility to which it is issued.

7.5 Respond to inquiries about an identifier's status including *(1)* whether it is valid based on examination of the check digits; *(2)* its status – not issued, active, retired; *(3)* when it was issued (and possibly the identity of the cooperating EMPI if usage policy permits this); and *(4)* if the identifier is unblindable, its current blinding status (not applicable, blinded, unblinded).

7.6 Define each new PVID class including the usage policies that apply to that class.

7.7 Establish the data items that need to be collected by the caregiver facility when requesting a VUHID identifier of any class (OVID or PVID), for example, the type of data, the type of facility, and the location of the facility.

7.8 Create a distributable electronic form to collect this information.

7.9 Provide upon request a description of the limitations and restrictions that apply to any particular class of private identifier.

7.10 Maintain the active/inactive status of each identifier.

7.11 Accept change of status indications from a cooperating EMPI for each identifier (active to retired/inactive, blinded to unblinded) and notify all cooperating EMPIs of these changes.

7.12 Issue the current status of a specific identifier on request.

7.13 Receive requests for clinical information from a cooperating EMPI relating to a specific identifier and distribute them to all cooperating EMPIs.

7.14 Log each clinical information request that is received and each identifier issued.

7.15 Issue code objects to print identifier cards for OVIDs and PVIDs.

7.16 Issue code objects to write OVIDs and PVIDs as 2D bar-codes.

7.17 Issue code objects to read OVIDs and PVIDs as 2D bar-codes.

7.18 Private identifiers that are intended to label blinded data may need to be unblinded. The VUHID will track the status of such identifiers to indicate if they are still blinded or have been unblinded.

8. Functions NOT Supported by the VUHID Facility

8.1 Storage of demographic, personal identifying, or clinical information associated with any identifier.

8.2 Providing the identity of an individual associated with any identifier.

8.2.1 A cooperating EMPI facility may support this function as long as it is consistent with the usage policy for that class of PVID or the identifier is an OVID.

8.2.2 An example of the need for this function is unblinding of research results at the end of a particular study. This would be supported by issuing a PVID class specifically designed to support this activity.

9. Identifier Principles

9.1 A VUHID identifier (both OVIDs and PVIDs) has the following syntax:

9.1.1 Prefix – 16 digits

9.1.2 Delimiter – a period "."

9.1.3 Check digits – 8 digits

9.1.4 Privacy digits – 7 digits

9.1.5 Total identifier – 32 characters in length

9.2 An identifier represents an OVID if, and only if, all of the privacy digits are zero. If any privacy digit is non-zero then the identifier is a PVID. Here are two examples:

9.2.1 OVID: 1234567890123456.123456780000000

9.2.2 PVID: 1234567890123456.926538261234567

9.3 Note that for purposes of brevity leading zeroes and trailing zeros that are privacy digits can be omitted so that 58206305.416389065892 is a valid identifier. (Trailing zeros that are check digits cannot be omitted.)

9.4 An identifier can be represented as a character string with a length of up to 32 digits and also as a 2D bar code using the AIIM Standard PDF417 bar code format.

9.5 Creation of other forms of representation of a VUHID, such as a magnetic stripe, is also permitted.

9.6 It should be feasible to enter a VUHID identifier using a telephone keypad. Either the '*' or '#' keys may be used to represent the delimiter.

9.7 Each VUHID identifier must be considered to be an atomic item. It is not permitted to print, manipulate, represent, process, or otherwise handle just a portion of an identifier. Specifically, it is not valid to isolate the prefix portion and attach it by itself to a document or electronic file.

9.8 A VUHID identifier (both OVIDs and PVIDs) can only have one of two statuses: 'active' or 'inactive'.[4] An identifier is marked as active when it is issued and it is marked as inactive when a valid request to do so is received by the VUHID facility from a cooperating EMPI facility. Any cooperating EMPI can request the current status of a specific identifier at any time as needed.

[3] For model contract language that might form a basis for the development of a VUHID contract, see http://www.connectingforhealth.org/commonframework/model_contract.html.

[4] It is possible that a third category of 'indeterminate' may be needed, for example if the VUHID receives a status request about an identifier that has not yet been issued, or that is of a certain privacy class with restrictive privacy requirements.

9.9 Each time an automated system receives a VUHID identifier the system must examine the check digits to verify that it is a valid identifier. This verification must be performed prior to any storage or use of that identifier.

9.10 An identifier that fails validation will be deemed invalid and discarded. This can lead the receiving system to issue a request for reentry and/or resubmission of the identifier information.

9.11 The prefix portion of a VUHID identifier is unique only within its given privacy class. Each complete VUHID identifier is unique but the characters composing the prefix component are not unique across various privacy classes. Thus:

9.11.1 12345.123456780000000, and

9.11.2 12345.123456781000000 are two entirely independent identifiers that apply to two different persons. The first is an OVID and the second is a PVID of class 1000000. The fact that the prefix is identical in the two VUHID identifiers does not by itself have any significance. Specifically it does NOT mean that they apply to the same person.

9.12 Any leading prefix or trailing privacy class zeros or both in this string may be omitted for display purposes in order to make the identifier more compact but any zeros in the 'interior' of the identifier or zeros that occur in the check digits must be retained to preserve the integrity of the identifier. Thus both 0000057290683608.275094639350000 and 57290683608.27509463935 are valid representations of the same identifier.

9.13 To facilitate zero suppression of long PVIDs, new PVID classes will be defined and issued in a manner that makes possible as much zero suppression as possible for as long as is feasible.

9.14 For example, the first privacy class should be 1000000 rather than 0000001 and the second should be 2000000 rather than 0000002.

9.15 *Delimiter Requirements:*

9.15.1 The delimiter must be printable in all language type fonts.

9.15.2 It must be clearly distinguishable from all numeric digits.

9.15.3 Should be easily visible, "." may be overlooked or not print well.

9.15.4 ";" or ":" or "*" or "$" or "@" or "#" are acceptable alternatives to ".".

9.15.5 The space character is not a valid candidate to serve as the delimiter character.

10. Identifier Presentation

10.1 A VUHID identifier can be represented in one or more of three forms:

10.1.1 A character string that is human-readable. (Note that suppression of leading and trailing zeros as described in section 9.12 is permitted.)

10.1.2 A bar-code representation that is a faithful representation of the complete 32-character identifier string.

10.1.3 A magnetic stripe representation of the complete identifier character string.

10.2 Additional VUHID identifier representations such as smart cards may be permitted as determined by the VUHID managing organization.

11. Identifier Cards

11.1 Patients receiving a new VUHID identifier will be issued an ID card printed with both the character and bar code representations. For OVIDs the patient's name may also be printed on the ID card. For PVIDs the patient's name and any other identifying demographic information would NOT be printed on the card in order to preserve privacy should the card be lost.

11.2 OVID identification cards provided to a patient should be printed with a white paper background.

11.3 Printed versions of PVID identifier cards should be differentiated in some consistent manner, for example, using a colored card background, to make it clear that they represent private identifiers.

11.4 The word 'private' should be prominently displayed on each PVID card.

11.5 VUHID identifiers on printed documents:

11.5.1 An OVID may be printed on a document that also contains patient-identifying information such as name and demographics.

11.5.2 A PVID may NOT be printed with any associated patient name, patient demographics or any other patient-identifying information on the document.

11.6 For both OVIDs and PVIDs a bar code representation of the identifier may be accompanied, if desired, by a printed character representation of the identifier underneath the bar code as well.

11.7 Representation of OVIDs and PVIDs on laminated cards, credit-card formats, smart cards, magnetic stripes, and other media may be supported if approved by the VUHID managing organization.

12. Requesting an Identifier

12.1 A high-level diagram showing the sequence of events to request a new OVID identifier is shown in Fig. 1.[5]

12.2 *Issuing a New OVID:*

12.2.1 The patient requests issuance of an 'open' identifier from their healthcare provider.

12.2.2 The healthcare provider's staff collects the required demographic information to unambiguously identify the patient and sends this to the cooperating EMPI facility. The demographic information collected must be of sufficient scope and quality to ensure adequate confidence in the resulting EMPI match for the person.

12.2.3 The cooperating EMPI facility does a demographic match to identify the patient.

12.2.4 If the patient is not known to the EMPI it uses the demographic data to register the patient.

[5] The intent is that a new VUHID identifier can be rapidly (within a few minutes at most) issued whenever it is needed and in any care setting that is participating as part of a cooperating EMPI system.

OVID Issuance

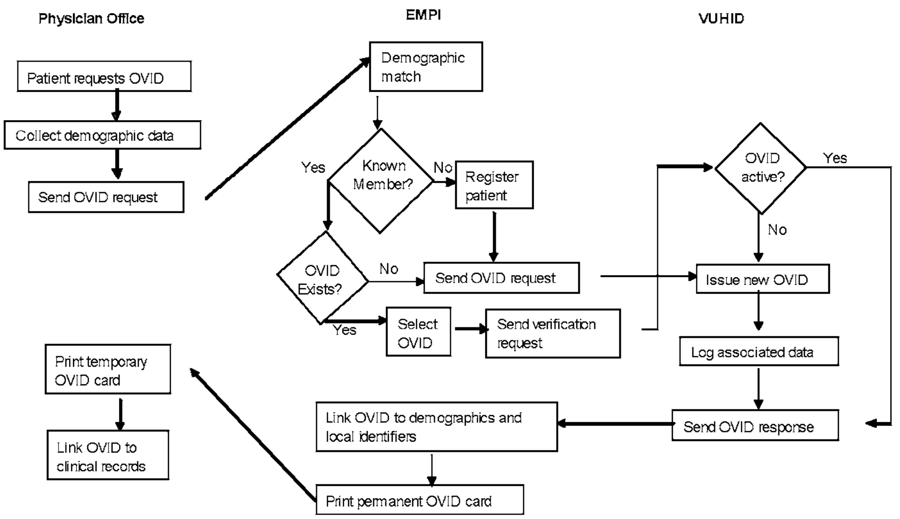

FIG. 1 OVID Issuance

12.2.5 If the patient is known to the EMPI facility it checks to see if the person already has an OVID. (The patient may have forgotten that they registered previously.)

12.2.6 If the cooperating EMPI determines that the patient does have an OVID, it queries the VUHID to determine that it is still active and, assuming that it is, the OVID is returned to the requesting healthcare provider. If the OVID identified by the EMPI is not active, the EMPI requests that the VUHID issue a new OVID for the patient to use.

12.2.7 If the EMPI determines the patient does not have an OVID identifier the demographic data is retained by the EMPI facility and a request for issuance of an OVID is sent to the VUHID.

12.2.8 The VUHID verifies the identity of the cooperating EMPI, issues a new unique OVID,[6] logs the time and the identity of the cooperating EMPI associated with this OVID and notes this OVID as being 'active'.

12.2.9 The OVID is returned to the cooperating EMPI system.

12.2.10 The cooperating EMPI system links the OVID with the patient's demographic information and with local identifiers associated with that patient, prints out a laminated card containing the patient's name, OVID character string and the corresponding bar code to be mailed to the patient, and sends the OVID to the healthcare provider.

12.2.11 A temporary paper copy of the OVID is printed in the physician's office and given to the patient along with brief instructions for its use.

12.2.12 The physician's staff has the option to use the OVID to directly identify and link medical information associated with that visit as well as any previously existing information associated with that patient.

12.3 *Issuing a New PVID:*

12.3.1 The patient requests issuance of an identifier from their healthcare provider's office staff and indicates they wish this information to be kept confidential *or* the provider's staff may know that the information to be covered is of a nature that requires confidentiality (for example, this is a psychiatric facility).

12.3.2 The physician's staff obtains the patient's OVID[7] or the required demographic information to identify the patient to the cooperating EMPI.

12.3.3 The staff also collects (using a form generated by the VUHID and downloaded from the cooperating EMPI facility) the additional information needed to describe the privacy aspects of this clinical episode—type of clinical information that will be processed, type of facility, location, etc.

12.3.4 The staff sends both *(1)* the OVID or demographic identifying information and *(2)* the privacy descriptive information to the cooperating EMPI.

12.3.5 The cooperating EMPI facility uses the OVID, if one is provided, to identify the patient or otherwise does a demographic match to identify the patient.

12.3.6 If the patient is not known to the EMPI, it uses the demographic data to register the patient.

12.3.7 If the patient is known to the EMPI, it checks to see if the person already has an active PVID (the patient may have forgotten that they previously obtained one) covering this

[6] Note that, for purposes of fraud detection, the prefixes of the OVIDs and PVIDs issued by the VUHID will not be issued in numeric order but will be issued in a random sequence. Thus, given one, or even a set, of prefixes, it is not possible to conclude what the prefixes of other valid VUHID indentifiers might be.

[7] Note that it is a policy decision, yet to be determined, whether a person requesting a PVID should be required to have an OVID first. If this is determined to be the case, then a request to issue a PVID would automatically also result in the cooperating EMPI requesting the issuance of an OVID if the person does not yet have one.

situation. (If a PVID exists, the EMPI checks with the VUHID to confirm it is still active.)

12.3.8 If the patient has an appropriate active PVID, it is returned to the requesting physician's office.

12.3.9 Otherwise, the demographic data/patient identity is retained by the EMPI and a request for issuance of a PVID is sent to the VUHID accompanied by the descriptive information describing the privacy requirements of this particular episode.

12.3.10 The VUHID verifies the identity of the cooperating EMPI, determines what class of PVID is appropriate, issues a new PVID of that class, logs the time and the identity of the cooperating EMPI associated with this PVID and notes this PVID as being 'active.'

12.3.11 The PVID is returned to the cooperating EMPI system together with an electronic document describing the usage restrictions for this class of PVID.

12.3.12 The cooperating EMPI system links the PVID with the patient's demographic information, prints out a laminated card containing the PVID (but *not* the patient's name) and a corresponding bar code representation together with a paper copy of the usage restrictions to be mailed to the patient, and sends the PVID to the physician's office with an electronic copy of the usage restrictions.

12.3.13 A temporary paper copy of the PVID is printed in the physician's office along with a copy of the usage restrictions and given to the patient.

12.3.14 The physician's staff use the PVID to identify medical information associated with that visit and can use the PVID to link any similar previously existing information associated with that patient that would also fall under the usage restrictions of this particular class of PVID.

13. VUHID Implementation Principles

13.1 The VUHID system should be implemented in a manner that ensures security and high availability on the Internet.

13.2 The VUHID facility must be equipped with backup and failover capabilities to ensure continuous 24/7 availability.

13.3 The Internet server supporting the Internet interface will be separate from the server supporting the VUHID database for security and data integrity reasons.

13.4 The VUHID facility will only issue one identifier in response to each request from a cooperating EMPI.

13.5 The VUHID server should have sufficient capacity to consistently ensure sub-second response time.

13.6 Each identifier issued by the VUHID must be guaranteed unique.

13.7 There shall be no reuse of identifiers. An identifier that is marked as inactive is permanently retired.

13.8 Secure, encrypted communications channels must exist between the VUHID facility and each of the cooperating EMPI facilities.

13.9 The VUHID facility will *only* communicate with cooperating EMPIs.

13.10 The VUHID facility will *never* store personal demographic, identification or clinical information.

13.11 It will store information identifying each cooperating EMPI system.

13.12 It will log the date & time, and identity of the requesting cooperating EMPI system for each VUHID identifier that is issued.

13.13 An OVID can be provided to whomever requests it via a valid cooperating EMPI request.

13.14 A PVID can be provided only under the appropriate circumstances associated with its privacy class. The request for issuance of a PVID must contain sufficient descriptive information concerning the privacy requirements for the VUHID to accurately determine the appropriate class of PVID that should be issued.

13.15 The VUHID can be queried to determine the active/inactive status of an identifier. Valid responses include: active, inactive, or not yet issued.

13.16 Requests for patient clinical information can be submitted to the VUHID via a cooperating EMPI for distribution to all cooperating EMPI systems. It is the responsibility of the EMPI to perform adequate verification of the identity and authorization of the requesting clinician.

13.16.1 The request must include a valid VUHID identifier.

13.16.2 The request must describe the types/categories of information required.

13.16.3 The request must indicate the location (URL) to which results will be sent. (Note that none of the information will be sent to the VUHID. Instead it will be sent directly to the requesting party.)

13.16.4 The request must be logged by the VUHID facility.

13.17 The VUHID will maintain the status (active or inactive) of each identifier.

13.17.1 An identifier will be marked as active when it is issued.

13.17.2 A cooperating EMPI can send a message indicating that an identifier should be made inactive.

13.17.3 A cooperating EMPI can query the status of a specific identifier whenever and as often as needed.

13.17.4 The VUHID will log the date on which an identifier becomes inactive and the identity of the cooperating EMPI which indicated this status change.

14. How a Patient/CDO Uses a VUHID Identifier Once It Has Been Issued

14.1 Note that VUHID identifiers issued to the same person will each have a different prefix in order to preserve the anonymity of PVIDs. If each VUHID identifier for a person had the same prefix component then it would not be possible for the identifiers to serve their anonymization function because anyone knowing the identity of a person associated with one prefix component would immediately know the identity of the person associated with all other VUHID identifiers that had the same prefix component.

14.2 *OVID Sample Uses:*

14.2.1 A patient that has received an OVID from a physician's office would present the OVID at the next visit. The staff would use a bar code reader to read the OVID and would retrieve the patient's demographic information (ideally from the cooperating EMPI but this could be from a local physician's office automation database.) The staff would verify that the patient is correct and that none of the information has changed (new cell phone number, new address, new name due to marriage, new insurance carrier, etc.). If there happens to be new/updated information the staff captures the changes and passes them along to the cooperating EMPI so that its database is appropriately updated. The patient would not have to provide any further demographic information during the visit.

14.2.2 The patient goes to another physician's office after receiving their OVID. The second physician's staff read the OVID using a bar code reader and request the associated demographic and insurance information from the cooperating EMPI. The staff person verifies the patient's identity by checking a few key items and then uses the downloaded information to update the local system. Again, the patient does not need to supply demographic information.

14.2.3 Essentially the same sequence would apply if the patient visited any other facility that is associated with the cooperating EMPI.

14.2.4 In a situation where a physician has minimal office automation but does have internet connectivity the office staff person could enter the OVID (typing or bar code reader) and send the request to the cooperating EMPI. In response they would receive a printed copy of the relevant demographic/ insurance information and could use this to complete their records.

14.3 *PVID Sample Uses:*

14.3.1 PVIDs would be used in a manner roughly analogous to OVIDs but have additional restrictions associated with the specific privacy class for the particular PVID being used. Each PVID class is meant to serve as a linkage mechanism for a set of information that must operate under a specific set of operational constraints that are different from those of any other PVID class. The factors that determine these unique constraints are not fully definable at this time but are anticipated to include such factors as *(1)* the nature of the data (psychiatric data will need to be treated differently from sexually transmitted disease data), *(2)* the governing legal jurisdiction (different states will have different regulations applying to the same types of information), *(3)* special conditions (research), and *(4)* patient preferences.

14.3.2 Mr. Jones has his initial visit with a psychiatrist. Because of the nature of this clinical information the psychiatrist uses Mr. Jones's OVID to request issuance of a PVID for linkage of psychiatric data. Depending on policy and operational issues the issued PVID may or may not be linked to the OVID by the cooperating EMPI but in either case the PVID is what is used to identify information in the psychiatrist's office.

14.3.3 Later, Mr. Jones is seen by his physician who suspects the possibility of AIDS. In order to protect the privacy of this information the physician requests a PVID of a different privacy class via the cooperating EMPI to be used to identify the AIDS laboratory test and its result independent of Mr. Jones's other clinical information.

14.3.4 Mr. Jones is admitted to a hospital for routine surgery. Because he is considered to be a VIP the hospital requests issuance of a PVID from yet another privacy class to be used to shield his identity during this hospital stay.

14.3.5 During this hospitalization the hospital also requests a separate PVID to be used exclusively for billing purposes. This protects Mr. Jones's identity when billing procedures are being executed whether the hospitalization is being tracked using an OVID or a PVID for clinical information linkage.

14.3.6 Mr. Jones grants permission for his clinical information to be used in a blinded clinical trial where the data collection and analysis need to be performed in a blinded fashion but eventually the results need to be unblinded for subsequent follow up. Again, a PVID of a particular privacy class is issued for purposes of information linkage during the research study with the understanding that the principle investigator will be permitted to unblind this particular set of PVIDs when the proper conditions are met at the end of the study.

15. Multiple People Using the Same Identifier

15.1 The identifiers issued by the VUHID will each be unique. At the present time, however, there are no known mechanisms to actively prevent multiple people from attempting to use the same identifier even though this is a violation of the principles of the VUHID system. It is hoped that mitigating factors such as *(1)* the ease of obtaining a VUHID identifier, *(2)* the anticipated low cost of these identifiers, and *(3)* the fact that anyone wishing to have such an identifier need only request one from a physician participating with a cooperating EMPI will make the incidence of multiple people trying to use the same identifier quite low. It should be a major point of the patient education which occurs when an identifier is issued to make it clear that there is no need for multiple people to use the same identifier and indeed there are significant risks to doing so.

15.2 Despite this, it is likely that situations will occur where a physician or a cooperating EMPI will detect that multiple people have used the same VUHID identifier to aggregate their medical information either intentionally or unintentionally. When this situation is discovered a notification should immediately be sent via the cooperating EMPI to the VUHID to have that identifier made inactive. Requests should then be sent by the cooperating EMPI to have a new replacement identifier of the same privacy class (OVID or PVID) issued for each person involved. The cooperating EMPI must then address the issue of trying to separate the various items of medical information attached to the now-inactive previous identifier in order to reassign correct linkages for that information to one of the newly issued identifiers.

16. Multiple OVIDs Used by a Single Person

16.1 In the ideal situation, each person would have a single OVID (although they might have multiple PVIDs for various uses.) However, there is no mechanism to actively prevent a person from obtaining multiple OVIDs. While this is not a desirable situation, it should be possible for a cooperating

EMPI to link together multiple OVIDs relating to the same person and be able to link them in such a manner that relevant clinical information can be associated with all of them so that it does not matter which specific OVID is used for a particular clinical encounter.

17. Temporary Identifiers

17.1 A specific class (yet to be determined) of PVIDs will be designated for use as temporary identifiers. These identifiers can be requested by a care delivery organization for use as an identifier when treating a patient whose identity cannot be determined for whatever reason.

17.2 Information on the unknown person can be linked to the temporary PVID for as long as is necessary.

17.3 Once the identity (and corresponding VUHID identifier) of the patient is determined, then all information should be transferred to the valid identifier for that person. If the identified person does not have a permanent VUHID identifier then one should be issued once the identity of the person becomes known.

17.4 At that point the care delivery organization should retire the temporary identifier and notify the VUHID through its cooperating EMPI that the temporary identifier should be retired and converted to inactive status.

18. Cooperating EMPI Facilities

18.1 *Definition*—A cooperating EMPI facility is:

18.1.1 A site controlled by an organization dedicated to serve the matching and linking needs of a defined set of healthcare facilities and its members.

18.1.2 Capable of supporting a full set of EMPI functions.

18.1.3 Covers a minimum set of lives. The anticipated minimum is yet to be determined but is anticipated to be at least 1 million lives.

18.1.4 Maintains a demographic database.

18.1.5 Performs matching capabilities on demographic data.

18.1.6 Supports mapping capabilities across various identifiers and identifier categories.

18.1.7 Is able to map multiple OVIDs to an individual.

18.1.8 Is able to map multiple PVIDs to an individual under the restrictions that apply to each specific PVID class.

18.1.9 Implements VUHID functions in a way that supports the full scalability of VUHID identifiers (can support full 16-digit prefixes and 7-digit privacy classes).

18.1.10 Able to register new participants by providing a form which can be printed out by a care delivery organization (or a web site where the data can be entered) that captures the necessary demographic and clinical information needed to unambiguously identify the person and to determine the proper class of VUHID identifier needed.

18.1.11 Maintains any client-specific privacy/confidentiality requests agreed to with the patient.

18.1.12 Has a performance agreement with each of its participating healthcare facilities and tracks their existence and functionality.

18.1.13 Has a performance agreement with the VUHID facility to operate according to the principles of this implementation guide.[8]

18.1.14 Is able to maintain appropriate security and privacy of clinical and demographic information.

18.1.15 Is able to meet appropriate performance requirements for response time, availability, business continuity and disaster recovery.

18.1.16 Is able to maintain secure communications with the VUHID facility and with each of its participating healthcare facilities.

18.1.17 Is able to log all transactions.

18.1.18 Is able to handle requests from a participating healthcare facility for issuance of an identifier.

18.1.19 Is able to verify that the necessary information has been collected from a participating healthcare facility to request issuance of a given class of OVID/PVID and store that information linked to the identifier that is subsequently issued by the VUHID site.

18.1.20 Is able to store and provide on request, for each class of PVID, the associated rules and operational principles issued by the VUHID that govern that class of identifier.

18.1.21 Is able to handle requests from its healthcare facilities for clinical information residing outside the domain and return that information to the requesting facility once it is supplied by other cooperating EMPIs.

18.1.22 Is able to store locally or retrieve from an appropriate participating healthcare facility the current insurance coverage information relating to an individual (or at least a pointer to that information).

18.1.23 Is able to receive requests from other cooperating EMPIs for clinical information, distribute those requests to its appropriate participating care giving facilities and transmit the returned results to the requesting cooperating EMPI. (This ideally would occur because the cooperating EMPI keeps a log for each VUHID identifier of the facilities that have information linked to that identifier. Alternatively, it could broadcast each request for such information to all of its participating healthcare facilities.)

18.1.24 Is able to transmit a change in identifier status from active to inactive to the VUHID.

18.1.25 If it detects that more than one person has been using the same identifier for linkage, the cooperating EMPI must immediately send a request to the VUHID to inactivate that identifier and request the issuance of replacement identifiers of the same privacy class for each of the persons involved. It must then assist in properly reassigning existing medical information from the (now inactive) previous identifier to the correct new identifier for the person to whom the information applies.

18.1.26 Agrees to operate according to the principles outlined in this document.

18.1.27 Is able to support blinding and, in selective cases, unblinding of information.

[8] For model contract language that might form a basis for the development of a VUHID contract, see http://www.connectingforhealth.org/commonframework/model_contract.html.

18.1.28 Many cooperating EMPI facilities could be established as part of the core capabilities of a Regional Health Information Organization (RHIO). Others might be formed as a mechanism to serve a particular clinical population (for example, pediatrics) or a particular geography (for example, a state) or some other defined constituency (for example, a large employer).

18.1.29 Overlapping constituencies between cooperating EMPI facilities (e.g. one serving a state and another serving a large employer population where the two have some persons in common) is permitted as long as the cooperating EMPI facilities provide the communications and functions needed to resolve discrepancies, updates, redundant information, etc. between each other.

19. Continued Need for Demographic Matching

19.1 It should be noted that the existence of the VUHID system does not totally eliminate the need for demographic matching. Once a VUHID identifier has been issued to a patient, that identifier should become the primary means for linkage of information on that person, but there are still several circumstances in which the cooperating EMPI needs to perform a demographic match.

19.2 When a request for issuance of an identifier is being processed by the EMPI, it must do a demographic match to ensure that the patient does not already have a VUHID identifier. If the EMPI finds a matching record, it must check that record to see if an identifier(s) has already been associated with that person.

19.3 When a VUHID-registered person in one cooperating EMPI domain wants to associate data from a prior EMPI domain where he/she did not use a VUHID identifier, then the prior EMPI domain must do a one-time demographic match in order to associate the person's VUHID identifier with their records in the prior domain.

19.4 The same need arises in the case where a patient requests one VUHID identifier, moves to another cooperating EMPI domain and there requests a second VUHID identifier. In order to properly link the two VUHID identifiers, a demographic match must be performed. (Note that this match would only be performed once for any cooperating EMPI that has historical data on that person. As a result, it is reasonable to require a high degree of fidelity [and manual assistance if necessary] in the demographic match required to link the patient's historical information.)

19.5 A cooperating EMPI receives a request for historical data on a person who was treated at one of its participating organizations before the patient began using a VUHID identifier.

19.6 And perhaps most importantly, demographic matching will continue to be necessary for that (hopefully small) portion of the population that chooses not to participate in the VUHID system.

20. Functions of the VUHID Managing Organization

20.1 The managing organization (MO) oversees the personnel staffing the VUHID.

20.2 The MO works in conjunction with ASTM to establish the operational policies that govern the VUHID and its activities according to the principles outlined in this document.

20.3 The principles that guide policy decisions relating to the VUHID are confined to those that benefit healthcare and the MO assists in enforcing this focus.

20.4 The MO helps market the availability and benefits of the VUHID to its constituents, care providers, patients and the general healthcare industry.

20.5 The MO is the recipient and manager of grants and funds relating to VUHID operations.

20.6 The MO is responsible for overseeing the financial operation of the VUHID.

20.7 In the event that there are fees relating to VUHID functions, the MO would be responsible for establishing the amount of those fees.

APPENDIXES

(Nonmandatory Information)

X1. EXAMPLES OF POLICY DECISIONS RELATING TO THE VUHID

X1.1 In order to function properly, the VUHID facility and its activities must be guided by a large number of established policies. It is not the role of this implementation guide nor the VUHID staff to establish those policies. However, it is the contention of this document that the VUHID capability described in this document represents a robust infrastructure that can be used to implement a variety of policy decisions once those policies have been determined by the appropriate decision making bodies. Here is a representative list of some of the policy decisions that must be made in order to enable the VUHID to operate:

1. Must a patient have an OVID in order to be issued a PVID? (This requirement would need to be enforced by the cooperating EMPI.)

2. Who specifies the condition(s) under which an identifier is inactivated?

a. At the time or some set time after the patient dies.

b. At the time multiple patients are discovered to be using the same identifier.

c. When malfeasance, fraud, or other inappropriate activity relating to that identifier has been determined to have occurred.

3. Who establishes and what is the policy governing each new PVID class that is created?

4. When are two sets of policies sufficiently divergent that a new PVID class is required?

5. What kind of item will be given to the patient when a new OVID is issued—a piece of paper with the patient name and OVID printed on it, a laminated card, an embossed plastic card, a plastic card with a magnetic strip, a smart card, a bar code image, etc.?

6. What is the difference in the item issued to the person if the associated identifier is a PVID rather than a OVID?

7. Who is responsible for educating patients and caregivers concerning the proper use of OVIDs and PVIDs?

8. How are physicians and the staff of cooperating EMPIs trained?

9. Where and how should enforcement of proper use of VUHID identifiers be established and who will do this enforcement?

10. What should be the maximum response time to issue an identifier in response to a request with requirements which represents a new class of PVID? (Would it work to issue a temporary identifier while the new PVID class is being formed and then retire the temporary identifier once the new PVID is available?)

11. What mechanisms should be employed to convince and cajole other existing healthcare organizations, vendors and standards bodies to incorporate VUHID identifiers as supported data elements in their standards specifications?

12. What should be the long-term funding mechanism to support the VUHID? Should it be financially self-supporting? Should it be permanently non-profit?

13. Should there be any fees or charges associated with VUHID activities? For example, what, if any, charge should be established for issuing an OVID or a PVID?

14. Who is authorized to generate a request for clinical information to a cooperating EMPI and how should that request be formulated? What proof of identity and authorization should be required from the requesting individual?

15. What level of security is appropriate to protect the information stored in the cooperating EMPIs and in the VUHID?

16. Can facilities that are not automated (for example, a private physician office) participate in the VUHID system using entirely manual techniques?

17. How should the physician's need to know all information when treating a patient be balanced against a patient's desire to keep some of that information confidential through the use of PVIDs?

18. If a VUHID identifier is inactivated in error, is it permissible to 'reactivate' it or should a new identifier be issued for the person in this situation with their old information linked by the EMPI to the new identifier?

19. If the VUHID receives a request to inactivate a specific identifier from a participating EMPI, does it automatically do so? Does it notify the other participating EMPIs when an identifier is inactivated?

X2. FREQUENTLY ASKED QUESTIONS

1. Why propose a voluntary system?

Choosing a voluntary approach yields many advantages for the VUHID system. People who choose to participate may do so by simply indicating an interest in obtaining a VUHID identifier. People who choose not to participate will not in any way be coerced to do so. Because of this flexibility there is no need for "enforcement" at the point where identifiers are issued (to determine whether a persons 'qualifies' to participate) and this dramatically reduces the cost of the system. In addition, this approach makes it feasible to implement the system incrementally over time so there will be no deadlines mandating when a person must make a decision to participate or not.

2. What is the VUHID system?

The VUHID system consists of *(1)* a central VUHID facility that issues identifiers, *(2)* cooperating enterprise master person index (EMPI) facilities at each area which are set up to share medical information, and *(3)* the hospitals, clinics, physicians' offices, and other medical facilities that are associated with each of those EMPIs. The system is designed so that medical information resides in components 2 and 3 of this system but is never seen by the central VUHID site.

3. What benefits should I realize if I choose to participate?

The single most important benefit of obtaining a universal healthcare identifier is that it enables the healthcare system to assemble your medical information in a comprehensive and error-free manner. The existence of a VUHID identifier will enable your current caregiver to obtain the appropriate information concerning you, even if it is scattered across many locations around the country, as long as each of those locations participates in the VUHID system. A second major benefit will be convenience. When you go into your physician's office you simply present your identifier and they will be able to acquire your identifying information from the system's EMPI capabilities. You will no longer have to repeatedly give your name, address, phone number, Social Security Number (SSN), etc. A third major advantage is that you have much better protection against identity theft. Rather than having to repeatedly provide your name, address, birthdate, SSN, telephone number, etc. each time you wish to identify yourself to a new physician or request transfer of medical information, you simply provide your VUHID identifier. This means that your personal identity information is not placed at risk by being transmitted, used, and stored in multiple situations. If something inappropriate were to happen, your identifier—not your identity—would be at risk. An identifier can be replaced if necessary but your identity cannot. Finally, use of VUHID identifiers will permit you much better control of your clinical information through the use of multiple private identifiers which are designed to keep various aspects of your clinical information private.

4. Why are VUHID identifiers so long?

The VUHID identification system has been designed to ensure that it can operate indefinitely. It also needs to be able to function properly despite many potential different policy and management decisions that could be made in the future. As a result the VUHID identifiers have been designed to ensure that they have sufficient capacity to be able to function for the foreseeable future and hence each identifier is a fairly long character string.

5. Why would a patient want to participate in the VUHID system?

The VUHID system has been designed so that a patient may receive a VUHID identifier simply by asking for one from any physician participating in the VUHID system. There are no other restrictions such as needing insurance coverage or citizenship. It is anticipated that the cost to obtain an identifier will be minimal. In an ideal situation open identifiers will be free and private identifiers will be available for less than one dollar. The potential benefits for VUHID identifier use include more accurate and more convenient clinical care. VUHID identifiers also will facilitate patient participation in research and clinical trials without exposing the patient to possible fraud and identity theft risks. Use of the VUHID identifier is anticipated to be much more convenient for a patient then repeatedly providing your identification information. Finally, use of VUHID identifiers should give patients much more control of particular portions of their medical records such as psychiatric, or substance abuse information.

6. What if a patient chooses not to participate in the system?

Because the VUHID is a voluntary system, it is anticipated that some patients will choose not to participate. These patients will continue to receive medical services in a manner very similar to how the system operates today. Each time they have a medical encounter they will need to provide their identification in the form of name, address, telephone number, birth date, Social Security number, and other identifying information - what are commonly called “patient demographics”. Because this data will be collected repeatedly, it is subject to potential errors in data collection and these errors lead to the possibility of incorrect linkage of clinical information. In addition, the patient will be at some increased risk of identity theft because this information will be transmitted, used, and stored in many different places throughout the healthcare system. However, there will be no pressure on a patient to migrate from this mode of ‘demographic’ operation to a VUHID identifier. The only reason to make this change will be that the patient decides that they wish to do so.

7. What uses are there for private identifiers?

Private VUHID identifiers are designed to help patients keep various portions of their medical information private and separate from their “open” medical information. Each private identifier belongs to a specific class which defines how that identifier and its associated information should be used. With a private identifier, the goal is to permit medical information to be aggregated to the identifier without knowing the identity of the person involved. The VUHID system anticipates that each person will have one open identifier and many private identifiers for use in various healthcare situations. Another major use for private identifiers will be for research activities where information on large numbers of patients needs to be brought together for analysis but there should not be any way to identify specific patients in this database. Use of a private identifier will allow appropriate pieces of medical information to be brought together for each such study but it will not be possible to determine the identity of the individuals who have participated in the study.

8. What are the costs associated with VUHID participation?

The exact cost of obtaining a VUHID identifier has not yet been established; however, the goal of the system is to ensure that cost is not a barrier to any person’s use of these identifiers. In an ideal world, “open” identifiers will be issued at no cost and private identifiers will be issued at a cost of less than one dollar each.

9. When do I need to decide if I want to join the VUHID system?

Because the VUHID system is a voluntary system, there is no deadline on when you need to join. We anticipate that over time more and more people will become convinced of the value of joining the system, but there is no anticipated cut off date when people will no longer be able to request a VUHID identifier.

10. What if I join the VUHID system but later decide that I do not want to participate?

VUHID identifiers can be deactivated. If a patient decides for whatever reason to no longer participate in the system, they would simply indicate that to their physician and they would then revert to the same identification methods that they used prior to joining the VUHID system.

11. How do I actually obtain an identifier?

If your physician is participating in the VUHID network, you simply ask your doctor or his or her medical staff or both to have an identifier issued. If the identifier is going to be used to keep certain medical information private (that is, you need a private identifier) then you may be asked some additional questions to determine exactly what the intent of this private identifier will be. Note that the only way to obtain a VUHID identifier is to request one from a physician who is participating in the VUHID network.

12. Who runs the VUHID system?

The VUHID system will be managed by an organization—yet to be determined—that is dedicated exclusively to promoting good healthcare. There is a small staff dedicated to the operation of the technical components of the system, but the policies by which the system operates will be established by the managing organization.

13. How can I be sure that my privacy will be protected?

A major aspect of the design of the VUHID system has been to ensure that there is no possibility that it would ever represent a threat to a patient’s privacy. The central VUHID system issues its identifiers based on receiving an authentic request from one of its cooperating EMPI systems. This request does not identify you as a patient nor does it contain any of your clinical information. In other words, the central VUHID facility does not ever see any information concerning you as a specific patient nor does it create any kind of database that contains any identifiable patient information or any clinical information. Because this information is kept exclusively at the

EMPI facility associated with your physician there is no possibility that the VUHID system can jeopardize your identity or the privacy of your medical information.

14. What if I lose my identifier?

There are several possibilities depending on the specifics of the situation. It is relatively easy for the EMPI system to issue you another ID card so that you can continue to use your existing identifier. If there is any danger of loss of privacy or any indication of malfeasance, it is possible to inactivate the existing identifier and to ask the VUHID to issue a new one of the same class. The EMPI will then need to transfer your existing information from the previous identifier to the new one.

15. How will my identifier help ensure that my physicians will have my complete and accurate medical information?

It will take some time for existing clinical information systems to convert to using the new identifier. In the interim, the EMPI facility will cross-link your VUHID identifier to other identifiers that are already being used by various clinical facilities to identify you. Over time, it is anticipated that more and more of the information systems will be converted to use VUHID identifiers directly. In either case, the use of a VUHID identifier in conjunction with the EMPI facility will enable your physician to obtain complete and accurate clinical information based on your identifiers, not based on trying to match your demographic information, where mistakes can occur. The VUHID system is also designed so that a valid request for your clinical information can be made anywhere in the country where a physician is participating in the VUHID system. This will help ensure that, even if you need medical care in some area where you do not have an established relationship with a physician, you will still be able to acquire your medical information should it be required for an emergency situation.

16. How does having an identifier help protect me from identity theft?

As noted in previous responses, once you are issued a VUHID identifier, the automation systems will use that identifier as the way to obtain your clinical information. You no longer have to provide information to establish your identity, and for that reason there is a dramatically reduced possibility that anyone would be able to access your identity for inappropriate uses. For example, if a piece of paper containing a printout of information linked to one of your private identifiers were to be stolen, the thief would be unable to determine who that information described because your private identifier does not contain any information pointing directly to you or your identifying demographic data.

17. How does a VUHID identifier help me control the privacy of my medical information?

The VUHID system will issue private identifiers of a variety of different classes. For example, one private class might be used to link psychiatric information. Another class of private identifier might be used to link your information in a blinded research study. Yet another class might be used to associate information needed to prepare a proper bill for your latest hospital stay. Each of these private identifiers could be used by appropriate and authorized medical personnel to provide clinical services to you. However, none of these identifiers could be used by an unauthorized person to determine your identity. The intent of these multiple classes of private identifiers is to allow you as a patient to exercise control over the privacy of your clinical information.

18. What is the relationship between the VUHID system and the Federal Government?

There is no relationship between the proposed VUHID system and any federal agency. The system is designed so that it will operate independent of any federal oversight. One of the major reasons for designing the system in this manner is so each individual patient can have maximum confidence that the VUHID system exists exclusively to help ensure that each patient receives appropriate medical care based on accurate medical information.

19. What will my VUHID identifier look like?

While the exact plans for the format of a VUHID identifier card are not yet finalized, it is likely that a VUHID identifier will take the form of a laminated wallet-sized card that contains the VUHID identifier character string and a bar code representation of that identifier.

20. What other functions besides healthcare will the VUHID serve?

None. The VUHID is dedicated solely to serving the needs of healthcare.

X3. EVALUATION OF VUHID PROPOSAL

X3.1 Guide E1714 provides a total of 31 evaluation criteria for any proposed implementation of a universal healthcare identifier. This section provides an evaluation of the VUHID proposal against those criteria to provide a rough measure of its suitability as a universal healthcare identification system. In order to evaluate the VUHID proposal against each of the criteria in this guide, the following evaluation scale is used:

1—not supported or not compliant

2—minimally supported

3—inadequately supported

4—adequately supported

5—fully supported

X—cannot be evaluated (this attribute does not apply directly to the sample VUHID scheme)

NOTE X3.1—The numbers in this evaluation correspond to the subsections of Section 5 of Guide E1714.

X2.7.1 *Accessible: 4*—Identifiers are available as long as the provider taking care of the patient is a participant in a network with a cooperating EMPI.

X2.7.2 *Assignable: 5*—The VUHID scheme supports the creation of a new identifier whenever required. Actually making this service available when and where it is needed depends on how the system is implemented (the extent of the network, mechanism to request identifiers, etc.)

X2.7.3 *Atomic: 5*—VUHID identifiers are considered to be a single data item.

X2.7.4 *Concise: 4*—VUHID identifiers permit the suppression of leading and trailing zeros. The use of alphanumerics instead of just numeric digits would make the code more concise, but creates significant implementation difficulties.

X2.7.5 *Content-Free: 5*—VUHID identifiers contain no information relating to the individual it identifies.

X2.7.6 *Controllable: 4*—Only cooperating EMPIs will have the information needed to reveal the identity of a person associated with a private identifier.

X2.7.7 *Cost-Effective: 4*—The cost of implementing an entirely new system such as the VUHID will undoubtedly be substantial. However, it should be noted that *modifying* an existing identifier (for example, the SSN) to better serve as an identifier would entail substantially greater expense than the creation of the VUHID system.

X2.7.8 *Deployable: 5*—VUHID identifiers can be implemented by any method that can support numbers and one delimiter character.

X2.7.9 *Disidentifiable: 5*—The PVID scheme prevents identification of the associated individual. The variety of PVID privacy classes supported means that additional PVIDs can be created as appropriate.

X2.7.10 *Focused: 5*—The VUHID system has been designed exclusively with the needs of healthcare in mind.

X2.7.11 *Governed: X*—This is a policy question independent of the VUHID plan.

X2.7.12 *Identifiable: 5*—The cooperating EMPI systems will have a full set of demographic information to identify the person associated with each identifier.

X2.7.13 *Incremental: 5*—Nothing in the VUHID scheme should inhibit the gradual phased-in implementation of the system.

X2.7.14 *Linkable: 5*—A VUHID identifier can be used as an identifying item on paper or a variety of automated technologies. It can be used as a field in databases that link a variety of forms of information.

X2.7.15 *Longevity: 5*—There are essentially no known limitations to the VUHID scheme.

X2.7.16 *Mappable: 5*—Modern database systems should have no trouble mapping the VUHID identifiers bidirectionally with currently existing healthcare identifiers.

X2.7.17 *Mergeable: 4*—This will require a linkage at the trusted authority that indicates the equivalence of two identifiers. Additional linkages may be required at individual institutions. While the VUHID scheme does not directly support merging in its internal data structure, this should not represent any significant hurdle for the system as a whole.

X2.7.18 *Networked: 5*—There are no barriers to implementing the VUHID scheme over a computer network.

X2.7.19 *Permanent: 5*—The VUHID scheme has sufficient capacity to prevent the need for the reuse of identifiers.

X2.7.20 *Public: 5*—The VUHID is designed to be fully disclosable.

X2.7.21 *Repository-Based: 5*—VUHID identifiers can be stored readily in a variety of database systems.

X2.7.22 *Retroactive: 5*—Nothing in the VUHID scheme should prevent its retroactive assignment to any person.

X2.7.23 *Retirement: 5*—Retiring an identifier is a fully supported function of the VUHID facility.

X2.7.24 *Secure: 4*—PVIDs offer the basic mechanism to provide secure operations; however, most of this capability must rest with policies and procedures implemented by the trusted authorities.

X2.7.25 *Splittable: 2*—There is no inherent ability to support splitting in VUHID identifiers. Splitting for prospective data can be supported by assigning new VUHID identifiers to both of the two individuals involved and retiring the old identifier.

X2.7.26 *Standard: X*—Insufficient information on applicable standards exists to assess this question at this point.

X2.7.27 *Unambiguous: 4*—The VUHID system has a period as a delimiter. This may be difficult to see in some printed forms.

X2.7.28 *Unique: 5*—The VUHID system has the duty to ensure that each identifier is unique.

X2.7.29 *Universal: 5*—The capacity of the prefix is sufficient to accommodate the world's population, should that be desired.

X2.7.30 *Usable: 4*—There should be no barriers to automated processing of a VUHID identifier.

X2.7.31 *Verifiable: 5*—It is possible to be sure that a candidate VUHID identifier is indeed valid due to the embedded check digits. This should provide a 1 in 100 000 000 chance of a random number being accepted as a valid identifier. Of course, it would be possible to achieve even higher confidence by adding more check digits to the VUHID design.

X2.8 *Evaluation Summary*—A summary of the evaluation of the proposed VUHID scheme is given below. The table indicates the number of criteria listed in this guide that fall into each category of the evaluation scale. For the sake of clarity, a copy of the evaluation scale given at the beginning of this section is also included here:

1—not supported or not compliant
2—minimally supported
3—inadequately supported
4—adequately supported
5—fully supported
X—cannot be evaluated (this attribute does not apply directly to the sample VUHID scheme)

Evaluation Category	Number of Criteria
1	0
2	1
3	0
4	8
5	20
X	2