Proposed American National Standard/
American Dental Association

Standard No. 1111

Oral Dataset Interoperability Network (ODIN)

ADA American Dental Association®

2023

PROPOSED AMERICAN NATONAL STANDARD/AMERICAN DENTAL ASSOCIATION STANDARD NO. 1111 FOR DENTISTRY – ORAL DATASET INTEROPERABILITY NETWORK (ODIN)

FOREWORD

(This Foreword does not form a part of the Proposed ADA Standard No. 1111 for Dentistry - Oral Data Interoperability Network (ODIN).)

In 1992, there was interest in the standardization of clinical information systems related to electronic technology in the dental environment. After evaluating current informatics activities, a Task Group of the ANSI Accredited Standards Committee MD156 (ASC MD156) was created by the ADA to initiate the development of technical reports, guidelines, and standards on electronic technologies used in dental practice. In 1999, the ADA established the ADA Standards Committee on Dental Informatics (SCDI). The ADA SCDI is currently the group that reviews and approves proposed American National Standards (ANSI approved) and technical reports developed by the standards committee's working groups. The ADA became an ANSI accredited standards organization in 2000.

The scope of the ADA SCDI is:

> *"The ADA SCDI shall develop informatics standards, specifications, technical reports and guidelines and interact with other entities involved in the development of health informatics standards aimed at implementation across the dental profession."*

ADA Standard No, 1111 was prepared by SCDI Working Group 11.9 on Core Reference Data at the request of Gregory Zeller, chair of SCDI Subcommittee on Clinical Informatics. The co-chairs of SCDI Working Group 11.9 are Bryan Laskin and Mark Jurkovich.

PROPOSED AMERICAN NATONAL STANDARD/AMERICAN DENTAL ASSOCIATION STANDARD NO. 1111 FOR DENTISTRY – ORAL DATASET INTEROPERABILITY NETWORK (ODIN)

1 Rationale

The Oral Dataset Interoperability Network (ODIN) provides for the permissioning, data bundling, authentication and necessity validation for structured electronic data elements to support key information exchange among and between dental and other health care settings. This includes the bidirectional electronic sharing of essential patient demographic, dental and medical encounter data, as well as patient clinical data in a structured, computable format between dental or other health care venues. Currently there does not exist a consistent value set of information contained within Electronic Dental Records (EDRs) and the information that does exist is stored in multiple incompatible formats. Additionally, there is a lack of ability to provide for adequate authentication and necessity of data access. Information contained with the EDR is vital to providing quality care, however each stakeholder involved in caring for patients (dental, medical, payor, patient, guardian, etc) has specific intricacies associated with the data contained within the EDR. ODIN, therefore, critically defines these specific EDR data access, storage, transmission, and aggregation elements by stakeholder. Each stakeholder involved in caring for patients (dental, medical, payor, patient, guardian, etc) has specific data requirements and methodologies associated with the data contained within the EDR.

Using the Fast Healthcare Interoperability Resources (FHIR)[1], Health Level 7 (HL7)[2], Consolidated Clinical Document Architecture (C-CDA)[3], the expanded data elements and schema details within the ODIN Standard draft allow for more accurate, secure and simple packaging and transmission of dental specific datasets. Leveraging the combination of these data elements, a vendor can then generate a machine-interpretabe (Extensible Markup Language (XML)[4] describing content) as well as human-readable (Hyper Text Markup Language (HTML)[5] describing the presentation) Oral Health Continuity of Care Document (OH-CCD)[6] as detailed in *ADA Standard No. 1084 For Reference Core Data Set For Communication Among Dental and Other Health Information Syste*m[7].

To expand on the functionality of the information included in ADA Standard No. 1084 and to achieve coordinated electronic information exchange between clinical information systems, the core dataset that shall be transferred is defined by provider type, along with technical specifications for how to store, transmit and process these datasets. Transmission of the OH-CCD between clinical information systems can be achieved using existing healthcare transport standards including HL7 FHIR, Direct[8], IHE Secure Exchange of Dental Information[9] and USCDI[10], along with ODIN. ODIN expands the limited dental datasets included within previous Standards available for consistent interoperability, as well as develop more robust dental data exchange protocols to assist clinicians and patients in providing and obtaining higher quality and more complete information to assist in improving care outcomes.

2 Scope

This standard provides a technical specification to extract, process, format and transmit essential patients' demographic and dental/medical encounters and clinical data between one

dental information system to another dental or medical health information system supporting key authentication, data bundling, syntactic and semantic information exchange. Included is a list of pertinent data fields and data bundles from the dental record about patients that health information system vendors can reference to internally map and extract information from their proprietary dental information system's data schema.

3 Normative References

The following standards contain provisions, which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. Since all standards are subject to revision, parties to agreements based on this specification are encouraged to investigate the possibility of applying the most recent edition of the specification or standard listed.

ANSI/ADA Standard No. 1084 for Reference Core Data Set for Communication Among Dental and Other Health Information Systems.

"SNODENT Values and Benefit: Making the Dental EHR Meaningful." American Dental Association. Chicago, IL. Accessed February 14, 2017.
(Available from the American Dental Association, 211 E. Chicago Ave., Chicago, IL 60611 or www.ada.org).

"Extensible Markup Language in Medical Standard Documents." In AMA Manual of Style: A Guide for Authors and Editors, 11th ed. American Medical Association. 2021.
(Available from the American Medical Association, 330 N. Wabash Ave., Chicago, IL 60611-58 or Oxford Academic (oup.com))

Comma-Separated Values (CSV) MIME type Registration, RFC 4180.
(Available *from RFC Editor,* https://tools.ietf.org/html/rfc4180)

Digital Imaging and Communications in Medicine (DICOM)
*(*Available from the National Electrical Manufacturers Association or www.dicomstandard.org)

DirectTrust direct messaging
(available from DirectTrust, 1629 K Street NW Suite 300, Washington DC 2000 or www.directtrust.org)

Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules.

The Health Information Technology for Economic and Clinical Health (HITECH) Act.
(Available from the U.S. Department of Health and Human Services, www. HHS.gov)

HTML 5.X: A vocabulary and associated APIs for HTML and XHTML
(Available from the World Wide Web Consortium, www.w3.org)

HL7 Consolidated Clinical Document Architecture (C-CDA) Version 2.X.

HL7 Reference Information Model

HL7 Version 2.X

HL7 FHIR Release 4.X

HL7 Electronic Health Records Dental Health Functional Profile, US Realm - Release 1.01
(Available from Health Level Seven (HL7), 3300 Washtenaw Ave., Suite 227, Ann Arbor, MI 48104 or www.hl7.org).

IHE Secure Exchange of Dental Information (SEDI).
(Available from www.ihe.org)

ISO/IEC 9075-1 Information technology — Database languages — SQL — Part 1: Framework (SQL/Framework)

ISO/IEC 10918-1 ISO Information technology — Digital compression and coding of continuous-tone still images — Part 1: Requirements and guidelines.
(Available from the American National Standards Institute, 25 West 43rd St., New York, NY 10036 or www.ansi.org)

JavaScript Object Notation (JSON) Data Interchange Format. RFC 8259.
(Available *from* RFC Editor, https://tools.ietf.org/html/rfc8259)

LOINC® (Logical Observation Identifiers Names and Codes)
(Available from the Regenstrief Institute, https://loinc.org/)

NIST Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53
*(*Available from the National Institute of Standards and Technology, www.nist.gov)

NDJSON Specification. (n.d.). NDJSON Specification.
(Available from http://ndjson.org/)

Rector AL, The Interface between Information, Terminology, and Inference Models
(Available from Medinfo, www.medinfo.com)

Systematized Nomenclature of Medicine -Clinical Terms (SNOMED CT)
(Available from SNOMED International, www.snomed.org)

Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446 Internet Engineering Task Force.
(Available from https://tools.ietf.org/html/rfc8446)

Tu SW and Musen MA. Modeling data and knowledge in the EON guideline architecture.
(Available from Medinfo, www.medinfo.com)

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program
(Available from the Office of the National Coordinator for Health Information Technology, www.healthit.gov)

United States Core Data for Interoperability (USCDI).
(Available from the Office of the National Coordinator for Health Information Technology, https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.)

4 Terms and Definitions and Acronyms

4.1 Within this standard the following nomenclature will be used for the purpose of clarifying which elements of the standard are required, recommended or optional for implementation:

4.1.1
Shall
indicates a mandatory requirement to be followed (implemented) in order to conform (Synonymous with 'is required to' and 'must')
(Note: These are normative, must be included, and cannot be ignored)

4.1.2
Should
indicates an optional recommended action, one that is particularly suitable, without mentioning or excluding others. Synonymous with 'is permitted and recommended.

4.1.3
May
indicates an optional, permissible action. Synonymous with 'is permitted'.

4.1.4
USCDI data class and data element nomenclature
nomenclature that shall be used whenever possible when identifying USCDI covered information.

4.2 Definitions of Terminology and Acronyms Used in this Standard

4.2.1
Acute disease
disease that comes on rapidly, and is accompanied by distinct symptoms that require urgent or short-term care

4.2.2
Acute infection
infection characterized by sudden or rapid onset of disease, which can be resolved quickly by robust innate immune responses exerted by the host or, instead, may kill the host

4.2.3
Acute inflammation
immediate, adaptive response with limited specificity caused by several noxious stimuli, such as infection and tissue damage (tissue necrosis)

4.2.4
API
Application Programming Interface

4.2.5
API versioning
the practice of managing changes to an API and ensuring that these changes are made without disrupting clients

4.2.6
Batch
publish-subscribe REST API call that enables applications to request or update large chunks of data in one request

4.2.7
Biologically derived product
material substance originating from a biological entity intended to be transplanted or infused into another (possibly the same) biological entity

4.2.8
CBCT
Cone-beam Computed Tomography

4.2.9
C-CDA
Consolidated Clinical Document Architecture

4.2.10
CDT
Code on Dental Procedures and Nomenclature

4.2.11
Client credentials flow
server to server flow where there is no user authentication involved in the process

4.2.12
CSV
comma-separated values

4.2.13
Delta
variant of a direct request that enables applications to discover newly created, updated, or deleted records

4.2.14
Direct request
request-response REST API call

4.2.15
DMHS
Dental Medical History Summary

4.2.16
DSD
Dental Specific Data, data which is specific to the dental industry (for example, tooth number(s))

4.2.17
DSDs
Dental Specific Datasets - a set of data that is specific to the dental industry (for example, information included in a dental referral for endodontic treatment)

4.2.18
DSS
Dental Specific Summary

4.2.19
EDR
Electronic Dental Record; the elements that constitute the subset of patient health information which are considered part of the patient's electronic dental record

4.2.20
EHI
EHI is electronic Protected Health Information (ePHI) to the extent that it would be included in a designated record set.

4.2.21
ePDI
electronic personal dental information

4.2.22
ePHI
Electronic Personal Health Information

4.2.23
FHIR
HL7 Fast Healthcare Interoperability Resources (FHIR) standard defines how healthcare information can be exchanged between different computer systems regardless of how it is stored in those systems

4.2.24
HL7
Health Level Seven (HL7) refers to the Standard Development Organization (SDO) that develops Standards for transfer of clinical and administrative data between software applications used by various healthcare providers

4.2.25
Interoperability
ability of computer systems or software to exchange and make use of information

4.2.26
JSON
JavaScript Object Notation; an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and arrays. It is a common data format with diverse uses in electronic data interchange, including that of web applications with servers

4.2.27
LOINC
Logical Observation Identifiers Names and Codes

4.2.28
ODIN
Oral Dataset Interoperability Network

4.2.29
OH-CCD
Oral Health Continuity of Care Document

4.2.30
M2M
machine-to-machine (M2M) applications where the system authenticates and authorizes the app rather than a user

4.2.31
Medication
pharmacologic agent used in the diagnosis, cure, mitigation, treatment or prevention of disease

4.2.32
Necrotic conditions
conditions that lead to the death of cells or tissue through disease or injury

4.2.33
NDJSON
Newline Delimited JSON); a variant of the JSON format recommended for bulk transfers

4.2.34
NIST
National Institute of Standards and Technology Cybersecurity Framework

4.2.35
Patient preferred contact methodology (PPCM)
method of which a patient prefers to receive information from the dental provider; by way of either secure messaging, non secure text message, secure email, non secure email or phone call. All communications, both non secure and secure shall comply with existing Standards (including HIPAA) regardless of patient preference

4.2.36
Patient record matching
identification and linking of one patient's data within and across health systems in order to obtain a comprehensive view of that patient's health care record

4.2.37
Problem list
document that states the most important medical problems facing a patient

4.2.38
RCDM
Reference Core Data Model

4.2.39
Rampant caries
multiple caries lesions in the same patient, often used in association with early childhood caries or radiation caries[1]

4.2.40
Referential database
type of database structure that stores and provides access to data points to stored items of information that are related to one another

4.2.41
SNOMED CT
Systematized Nomenclature of Medicine - Clinical Terms, a systematically organized computer-processable collection of medical terms providing codes, terms, synonyms and definitions used in clinical documentation and reporting

4.2.42
SQL
Structured Query Language- a domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system

4.2.43
SQLi
Structured Query Language injection; An SQL injection attack that uses malicious SQL code for backend database manipulation to access private information

4.2.44
SSOT
Single Source of Truth - the practice of structuring information such that multiple sources of information can be identified and leveraged to create one more accurate source for all the data points, ensuring that everyone requiring the information is working with the same data

4.2.45
Sub dataset
subset of a dataset

4.2.46
TLS protocol
cryptographic protocol designed to provide communications security over a computer network

4.2.47
Tooth anatomy DSD
combination of both the Tooth Number DSD and Tooth Surface DSD

4.2.48
Traffic access control
data security process that enables organizations to manage who is authorized to access data and resources[1]

4.2.49
USCDI
United States Core Data for Interoperability, a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange

4.2.50
USCDI data class
aggregation of various data elements by a common theme or use case

4.2.51
USCDI data element
most granular level at which a piece of data is represented in the USCDI for exchange

4.2.52
Webhooks
way for applications to communicate with each other using ever-driven architecture

4.2.53
XML
Extensible Markup Language (XML) is a simple text-based format for representing structured information

4.2.54
XSS
Cross-site scripting - type of security vulnerability that can be found in some web applications

4.3 Reference Terminology Used Within This Standard

It is the intent of ADA Standard No. 1111 to align with USCDI and SNOMED CT[11]. Therefore implementation of ADA Standard No. 1111 should include reference terminology included within USCDI and SNOMED CT when possible.

Wherever there is a conflict between definitions of terminology within this Standard documentation and USCDI or SNOMED CT, USCDI definitions should be used as the referenced terminology of choice or by SNOMED CT with USCDI as the preferred definition wherever there is a conflict.

5.0 Background

Accessibility to a patients' electronic Protected Health Information (ePHI) is vital when a healthcare provider is treating a dental patient. Previously dentistry has relied on overarching medical Standards, yet there are obviously dental specific information and challenges that require the dental industry to take into account. Additionally, the defining a more specific interoperability Standard to be implemented within the dental industry allows for more detailed specifications, which will elevate accessibility and quality of dental care.

5.1 Appropriate Uses of This Standard

Dental and other healthcare professionals will recognize that this Standard is intended to fill only a limited range of information that can be transferred between providers. Other Standards may be more appropriate for different interoperable information. This is not intended to be an exhaustive detailing of all information that can be communicated between health care providers, but rather an alignment of particular set of electronic Personal Dental Information (ePDI) that is defined, as well as what shall, should and may be shared between specified provider types, along with how that information shall be treated at rest and in transit. Accounting for authentication and the medical necessity of information accessibility for the specified ePDI is also defined.

5.2 Principal Models in Developing Clinical Information Systems

The principal models in developing clinical information systems are detailed within American

National Standards Institute/American Dental Association Standard No. 1084 For Reference Core Data Set For Communication Among Dental and Other Health Information Systems. This Standard describes that in order to achieve interoperability, there needs to be three types of principal models for the design and development of clinical information systems (*See* ***Figure 1***)[7]:

A. Information/Data models represent the structure and relationship of the information to be stored in any system. Examples of such models are Health Level 7 Reference Information Model[12], and HL7 Electronic Health Records Dental Health Functional Profile[13];
B. Terminology/Ontology models represent the meaning of the information that is stored within any system. Example of such models are Systematized Nomenclature of Dentistry (SNODENT)[14] and Systematized Nomenclature of Medicine – Clinical Terms (SNOMED-CT)[11]; and
C. Inference/Problem solving models serve in decision support and represent the consequence and actions which follow from what is stored within the system. Examples of such models are Medical Logical Modules (MLMs)[15], and Prodigy[16].

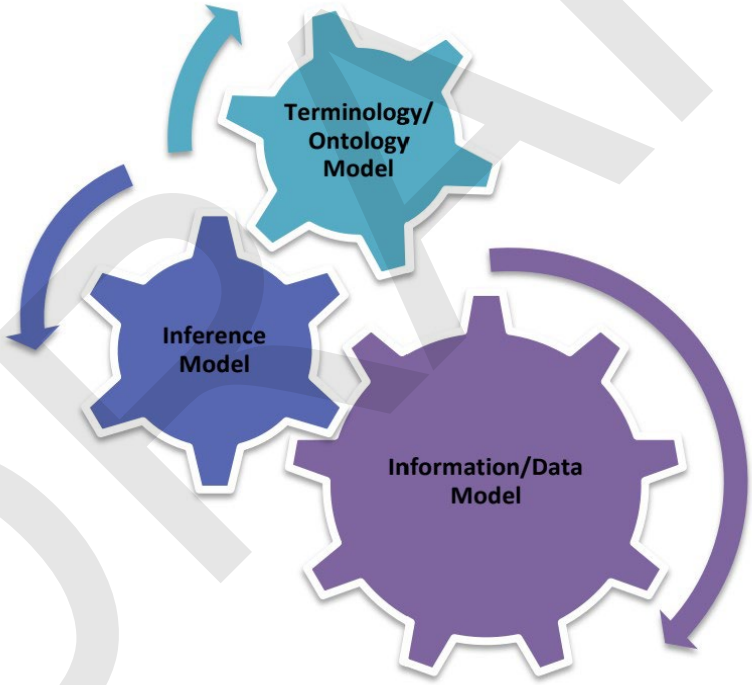

Figure 1: Three different types of principal models to achieve interoperability in clinical information systems[7]

ADA Standard No. 1111 ODIN defines data modeling for dental system informatics for specified data subsets that expand and organize the data defined within ANSI/ADA Standard No. 1084[17], referred to as the Reference Core Data Model (RCDM), as well as defines the data

model for dental specific information contained within the RCDM for the purpose of more accurate, easier to implement dental information interoperability. The information model for how to handle these datasets within transit, as well as accounting for user authentication and medical necessity is also described.

5.3 Principle Electronic Dental Patient Data Segments

A. Clinical Treatment Data represents the patient's ePHI and other electronic information that are used when providing clinical treatment of a dental patient. Examples of Clinical Treatment Data include electronic information that is sent between healthcare professionals when reporting treatment that will be or has been provided to that patient.
B. Business Operations Data represents the information regarding patient activity leveraged for marketing, sales, administrative or customer service purposes. Examples of Business Operations Data include marketing communications.
C. Payment Data represents the information used within the revenue cycle management of patient care. Payment Data includes insurance payments, patient payments and accounts receivable collection data.

ADA Standard No. 1111 ODIN defines Clinical Treatment Data modeling for electronic information exchange. Other Standards may define interoperability exchange for both Business Operations Data and Payment Data, which fall out of the scope of ADA Standard No. 1111.

6.0 Sub Datasets

A key component of developing meaningful interoperability between dental and other healthcare providers is categorizing the electronic data that is captured within a healthcare facility into useful sub datasets. While not comprehensive of all available sub datasets, the sub datasets in this section determine which sub datasets shall fall under the scope of this Standard for the purpose of treating the dental patient within healthcare provider interoperability.

For the purpose of clarity, sub datasets will be divided into several categories of information. While there may be some data that could be included in multiple categories, it is important to define each dataset into a specific category so that the information can be most useful for healthcare professionals and patients.

6.1 Single Source of Truth (SSOT)

As many data elements involved in caring for the dental patient can be sourced from multiple sources, it is difficult and likely not currently preferred to define a Single Source of Truth (SSOT). Therefore, conflictual information should be displayed for the overseeing healthcare provider to define the primary data to be referenced within the healthcare provider's EDR of a patient.

For example, if a patient has a reported history of diabetes at a medical facility, but reports no history of diabetes on the dental practice's medical history, the overseeing dentist may define whether or not the EDR referenced by that dentist reports a history of diabetes for that patient or not.

6.2 The Electronic Dental Health Record

Currently the vast majority of dental practices leverage a single software vendor that attempts to store the EDR. However EDR elements oftentimes come from sources external to this EDR vendor and can not write-back into the practice's EDR software. For example, new patient forms on a practice's website may contain a medical history that can not be directly imported into the patient's EDR.

Therefore, it is not appropriate to define the EDR as a single data source, but rather the aggregation and prioritization of multiple data sets into a SSOT, as described above.

The data elements that constitute the EDR are defined within ADA Standard 1084 and shall be treated as required by ADA Standard 1084, as well as other overseeing Standards and regulations, including this Standard, HIPAA[18], HITECH[19], and the ONC 21st Century Cures Act[20], including the most recent United States Core Data for Interoperability's (USCDI) standardized set of health data classes and data elements for nationwide, interoperable health information exchange. In order to avoid miscommunications, CDT and USCDI Data Class and Data Element nomenclature should be used whenever possible when identifying USCDI covered information. If there is a conflict in nomenclature, USCDI nomenclature is the preferred nomenclature of use within ODIN.

6.3 Non-Dental Record Electronic Patient Health Information

Through networking with healthcare providers both within dentistry and medicine more broadly, ODIN will obtain a combination of dental related ePHI, non-dental related ePHI from a patient, as well as elements that could be defined as both dental and non-dental ePHI (such as the patient's name and medical history). The categorization of ePHI as dental or non-dental may affect how the information is aggregated, organized and prioritized. Therefore, it is critical to define which data subsets are deemed dental and non-dental, as well as how to handle information that is covered and excluded within this Standard.

ODIN covered non-dental record ePHI includes the data elements that are obtained outside of ADA Standard 1084 (the defined EDR dataset) that is protected health information being saved, transferred or received in electronic form, including USCDI data elements. Therefore, the ePHI data management of this subset shall be treated as defined within this Standard document, as well as required by overseeing Standards and regulations, including HIPAA, HITECH and the 21st Century Cures Act. In order to avoid miscommunications, LOINC[21] and USCDI Data Class and Data Element nomenclature should be used whenever possible when identifying USCDI covered information.

6.4 ODIN ID: The Unique Patient Identifier Within Dentistry

While Unique Patient Identifiers (UPI's) exist within other interoperability Standards, such as FHIR, there is not a single UPI system developed within healthcare or within the current medical interoperability networks. This has led to the unfortunate reality where currently the primary complication that exists within data interoperability networks, including Health Information Exchanges (HIE's), is the inability to consistently and accurately match records for a patient. The fact that there is not a unique identification number or tag that acts as the core reference identifier for a patient further leads to an inability to create a SSOT for a patient.

Currently the most accurate form of Patient Record Matching is performed by developing referential integrity between ePHI containing referential databases via matching patient demographic information including patient date of birth, phone number, address, email address and other demographic information.[d, e] Creating a unique identifier for the dental patient, therefore, is not only feasible, but will act as a substantial step toward an ideally synchronized EDR set that could act, in the future, as a patient's EDR SSOT.

Just as it has been a challenge in developing a patient's accurate Electronic Medical Record due to the lack of a UPI, it is difficult, if not impossible, today to accurately identify and create a single EDR without the development of a UDI within dentistry. It is also difficult to join an individual's medical record with their dental record.

Additionally, the fact the datasets of a single patient's EDR, as defined within ADA Standard 1084[17], today rest in several systems, necessitate the creation of a Unique Patient Identifier (UPI) within dentistry, which will act as the referential database by which all the disparate datasets can be accurately attributed to an individual. For example, it is commonplace currently to have a single patient's dental history in a separate database from that patient's intraoral radiographs, while also having other elements of that patient's EDR in wholly other databases (such as CT scans, CAD/CAM scans, online forms, payment information, etc).

Therefore, for the purpose of consistent patient identification within ODIN and to provide accurate datasets within the line of dental care and administrative functions, all individuals shall be assigned a unique code to be used within dentistry called the ODIN ID. The ODIN ID shall consist of:

A. Twelve (12) digits
B. Example: 123456789012

Each ODIN provider shall ensure a single ODIN ID for each unique patient within their Dental EMR. The ODIN ID enables Patient Record Matching both within ODIN and through other interoperability Standards, most notably FHIR and USCDI. Therefore, any system leveraging ODIN shall perform accurate Patient Record Matching through the ODIN ID system.

When a new patient is entered for a dental encounter into an electronic health record (a

patient without an existing ODIN ID), an initial ODIN search should be performed to verify the patient demographic information is not within an existing ODIN ID. The patient demographic information to be searched includes, wherever possible, all Patient Demographics/Information as defined within USCDI and Patient Social Security Numbers.

A Patient Record Match will be determined to be positive if following data is found to be matching:

- First Name, Last Name, Current Address Zip Code and Date of Birth

When a Patient Record Match is found, the following available patient demographic information should be presented for verification, with matching patient demographic information presented in similar font and color, with mismatching patient demographic information presented in a contracting format (for example, red text color for mismatched elements vs black text for matching):

- First Name
- Last Name
- Current Address
- Date of Birth
- Administrative Gender (Sex as defined in USCDI)
- Phone Number
- Email Address

The overseeing healthcare provider should then have the option to edit any of the following, prior to matching / linking the patient record within the EDR to the ODIN ID:

- First Name
- Last Name
- Current Address
- Date of Birth
- Administrative Gender (Sex as defined in USCDI)
- Phone Number
- Email Address

Upon initial search of a new patient entered into an ODIN connected EDR, if a match is not made, the ability to edit or complete the above ePHI should be presented to the overseeing healthcare professional prior to the new ODIN ID being created within ODIN.

A referential database should be produced between ODIN and these interoperability Standards, such that ODIN ID's and UPI's can be manually linked and unlinked by an overseeing healthcare provider. All ODIN systems should, at least monthly, search for mismatched elements between ODIN and other connected USCDI interoperability Standards for each ODIN ID contained within the ODIN system. When a mismatch of the following available patient demographic information is found, the overseeing healthcare provider

should be presented with the mismatched patient demographic information for verification or editing with matching patient demographic information presented in similar font and color and mismatching patient demographic information presented in a contracting format (for example, red text color for mismatched elements vs black text for matching):

- First Name
- Last Name
- Current Address
- Date of Birth
- Administrative Gender (Sex as defined in USCDI)
- Phone Number
- Email Address
- Patient Preferred Contact Methodology (PPCM)

EHI consists of data elements that are not related to the health of a patient, yet are helpful in providing treatment, business operations or payment processing of the patient. This includes information including:

A. All USCDI Data Elements contained in USCDI Data Class Patient Demographics/Information
B. PPCM

All EHI should be structured and referenced as designated within USCDI and the FHIR Standards for interoperability wherever possible. Additionally the PPCM shall comply with existing privacy and security Standards (including HIPAA) regardless of patient preference and should be contained within the ODIN ID and verified as above.

6.5 Information Derived From The Electronic Dental Health Record Data

The data elements defined within ADA Standard 1084 may be used by a vendor solution to aggregate, combine or otherwise manipulate the elements to analytics or other insights into care provided. For example, failure rates of restorations, patient population demographic data and business intelligence metrics may be extrapolated by leveraging the data found within any database.

Information derived from the EDR which contains ePHI shall be treated as required by ADA Standard 1084, as well as other overseeing Standards and regulations, including HIPAA, HITECH and the 21st Century Cures Act.

7.0 Dental Specific Summary (DSS)

While DSDs are preferred when communicating within the dental profession as detailed above, oftentimes when communicating outside of the dental profession or in certain dental cases, it is preferred to have a summary of critical dental conditions. The purpose of the Dental Specific Summary (DSS) is to provide dental specific alerts for non-dental professionals

and for dental professionals that may not treat the overall patient, for example dental public health specialists.

The DSS shall not be used in replacement of any of the DSDs when communicating within the dental profession, however the DSS may also be included in addition to any DSDs. For example, when communicating with an Endodontist, the Endodontic DSD shall be included in the communication and the DSS may be included if deemed helpful.

DSS information should be included when a dental care provider is communicating with a provider requiring limited dental information and include the following conditions, as defined with the appropriate SNOMED identifier:

A. Rampant caries
B. Acute inflammation, infection or disease
C. Necrotic conditions

7.1 Dental Specific Data (DSD) and ePHI Medical Necessity Determination

Determination of medical necessity for all data, including Dental Specific Data within ADA No. 1111 ODIN is defined by overseeing Standards and regulations, including HIPAA, HITECH and the 21st Century Cures Act. Therefore any system leveraging ADA No. 1111 ODIN shall adhere to the restrictions contained within these Standards.

Consequently, business operations that are not in the line of care, involved with the active clinical treatment or payment processing of clinical treatment shall not have access to DSD and other ePHI. This includes past providers not actively in the line of care, officers and business staff members of a dental practice not involved in active clinical care or billing activities, as well as dental vendors, research institutions and other groups or Dental Service Organizations (DSO's) that are not actively involved in direct line of patient care or billing activities.

7.2 Dental Medical History Summary (DMHS)

As obtaining accurate medical history data is challenging for all providers, the following binary data elements shall be included in the medical history of a dental patient, as allowable through the USCDI (as defined within USCDI), CDT (Current Dental Terminology) and HL7 FHIR (Fast Healthcare Interoperability Resources) Standard workflow and as indicated as either "yes" as positive confirmation or "no" or "n/a" or left blank as negative or denial of a medical history of, as allowable by local, state and federal regulations, specifically regarding patient privacy:

A. Alcohol use Disorder
B. Alcohol abuse or dependence
C. Allergies and intolerances (including substances and reactions where available)
D. Biologically Derived Product (including organ transplants)

E. Cancer Care
F. Health Concerns
G. Hospitalization within the last 5 years (if available)
H. Medical Devices - Implantable Devices (including Unique Device Identifier where available)
I. Pregnancy Status
J. Smoking Status
K. Stroke/CVA
L. Substance Use

Additionally medical conditions that shall be included on the DMHS where available, along with last reported date include:

A. Autoimmune diseases
B. Bleeding illness
C. Breathing, lung or respiratory disorder
D. Cardiovascular disorder
E. Depression/anxiety
F. Diabetes
G. Frequent headaches
H. Gender Identity
I. Heart attack
J. Hepatitis
K. Administrative Gender (Sex as defined in USCDI)
L. Sexually Transmitted Infection
M. Stroke/CVA

7.3 Medical Problem List

The Problem List is a document that states the most important medical problems facing a patient. This typically includes a list of information that seeks to provide a current status of a patients' medical problems that require consideration or medical intervention. This includes information such as nontransitive illness or disease and injuries, as well as when there was resolution to the most current medical problems.

The EDR should incorporate accessibility of the EMR's Medical Problem List for an overseeing dental professional to access for a given patient when deemed necessary by that dental professional, if that Medical Problem List is available through the FHIR interoperability Standard.

7.4 Medications List

Most EMR's and EDR's maintain a list of patient medications, the Medications List. Each ODIN system should maintain a single Medications List for each ODIN ID as a Bundle FHIR document. A referential database of the Medications List should then be produced between

ODIN and other FHIR databases, such that ODIN and FHIR contained Medications Lists can be manually linked and unlinked by an overseeing healthcare provider. All ODIN systems shall, at least annually, search for mismatched elements between ODIN Medications Lists and other FHIR Medications Lists for each ODIN ID contained within the ODIN system. When a mismatch of the Medication Lists is found, the overseeing healthcare provider shall be presented with the mismatched Medications for verification or editing with matching Medications presented in similar font and color and mismatching Medications presented in a contracting format (for example, red text color for mismatched elements vs black text for matching).

7.5 Care Provider Electronic Information

When a two or more care providers are communicating electronically for the purpose of treating a dental patient, the information shall include:

A. Date of information sent or referral
B. Sending Office's Name
C. Sending Office's Address
D. Sending Office's Phone Number
E. Sending Office's Email Address
F. Sending Care Provider's (Dentist, Physician or care coordinator) Name
G. Receiving Office's Name
H. Receiving Office's Address
I. Receiving Office's Phone Number
J. Receiving Office's Email Address
K. Receiving Care Provider's (Dentist, Physician or care coordinator) Name

Care Provider Electronic Information shall be structured as referenced within the FHIR Standard.

7.6 Dental Specific Datasets (DSDs)

Information that is specific to dental treatment that shall be included when one dental care provider is communicating with another dental provider includes:

A. EHI
B. Data Bundles per provider, as indicated in Section 8 of this document

All DSDs shall be structured as either referenced within the FHIR Standard, the SNOMED Standard or as referenced within this document.

7.7 Tooth Nomenclature DSDs

Tooth Nomenclature DSDs shall be structured as referenced within the SNOMED Standard, using either the Universal or International tooth numbering system, with the data structured

as referenced within the FHIR Standard or within this document.

7.8 Tooth Surface DSDs

Tooth Surface DSDs shall be structured as referenced within the SNOMED Standard, with the data structured as referenced within the FHIR Standard or within this document.

7.9 Tooth Anatomy DSDs

Tooth Anatomy DSDs, the combination of both the Tooth Number DSDs and Tooth Surface DSDs shall be structured for interoperability as either referenced within the FHIR Standard, or as below:

7.9.1 Teeth

```
 {
   "tooth": {
      "system": "Snodent",
      "code": "161132D",
      "description": "Permanent upper left first molar tooth",
      "}
           surface": {
        "code": "MOD",
        "description": "Mesial-Occlusal Distal"
      }
   }
}

{
   "tooth": {
      "system": "Universal",
      "code": "14",
      "description": "Permanent upper left first molar tooth",
      "surface": {
        "code": "MOD",
        "description": "Mesial-Occlusal Distal"
      }
   }
}

{
   "tooth": {
      "system": "ISO",
      "code": "26",
      "description": "Permanent upper left first molar tooth"
      "surface": {
```

```
        "code": "MOD",
        "description": "Mesial-Occlusal Distal"
      }
  }
```

7.9.2 Segments

```
{
  "segment": {
    "code": "U",
    "description": "Maxillary"
  }
}
{
  "segment": {
    "code": "L",
    "description": "Mandibular"
  }
}
```

7.9.3 Quadrants

```
{
  "quadrant": {
    "code": "UR",
    "description": "Maxillary Right"
  }
}
{
  "quadrant": {
    "code": "UA",
    "description": "Maxillary Anterior"
  }
}
{
  "quadrant": {
    "code": "UL",
    "description": "Maxillary Left"
  }
}
{
  "quadrant": {
    "code": "LR",
    "description": "Mandibular Right"
  }
}
{
```

```
  "quadrant": {
    "code": "LA",
    "description": "Mandibular Anterior"
  }
}
{
  "quadrant": {
    "code": "LL",
    "description": "Mandibular Left"
  }
}
```

7.9.4 Surfaces

```
[
 {
  "surface": {
   "code": "D",
   "description": "Distal"
  }
 },
 {
  "surface": {
   "code": "DF",
   "description": "Distal-Facial"
  }
 },
 {
  "surface": {
   "code": "DFI",
   "description": "Distal-Facial Incisal"
  }
 },
 {
  "surface": {
   "code": "DFIL",
   "description": "Distal-Facial Incisal Lingual"
  }
 },
 {
  "surface": {
   "code": "DL",
   "description": "Distal-Lingual"
  }
 },
 {
```

```
  "surface": {
   "code": "DO",
   "description": "Distal-Occlusal"
  }
 },
 {
  "surface": {
   "code": "DOF",
   "description": "Distal-Occlusal Facial"
  }
 },
 {
  "surface": {
   "code": "DOL",
   "description": "Distal-Occlusal Lingual"
  }
 },
 {
  "surface": {
   "code": "DOLF",
   "description": "Distal-Occlusal Lingual Facial"
  }
 },
 {
  "surface": {
   "code": "F",
   "description": "Facial"
  }
 },
 {
  "surface": {
   "code": "FO",
   "description": "Facial-Occlusal"
  }
 },
 {
  "surface": {
   "code": "FOL",
   "description": "Facial-Occlusal Lingual"
  }
 },
 {
  "surface": {
   "code": "I",
   "description": "Incisal"
  }
```

```
},
{
 "surface": {
  "code": "L",
  "description": "Lingual/ Palatal"
 }
},
{
 "surface": {
  "code": "M",
  "description": "Mesial"
 }
},
{
 "surface": {
  "code": "MDFIL",
  "description": "Mesial-Distal Facial Incisal Lingua"
 }
},
{
 "surface": {
  "code": "MFD",
  "description": "Mesial-Facial-Distal"
 }
},
{
 "surface": {
  "code": "MFI",
  "description": "Mesial-Facial Incisal"
 }
},
{
 "surface": {
  "code": "MFIL",
  "description": "Mesial-Facial Incisal Lingual"
 }
},
{
 "surface": {
  "code": "ML",
  "description": "Mesial-Lingual"
 }
},
{
 "surface": {
  "code": "MLD",
```

```
    "description": "Mesial-Lingual-Distal"
   }
  },
  {
   "surface": {
    "code": "MLF",
    "description": "Mesial-Lingual-Facial"
   }
  },
  {
   "surface": {
    "code": "MO",
    "description": "Mesial Occlusal"
   }
  },
  {
   "surface": {
    "code": "MOD",
    "description": "Mesial-Occlusal Distal"
   }
  },
  {
   "surface": {
    "code": "MODF",
    "description": "Mesial-Occlusal Distal Facial"
   }
  },
  {
   "surface": {
    "code": "MODLF",
    "description": "Mesial-Occlusal Distal Lingual Facial"
   }
  },
  {
   "surface": {
    "code": "MOF",
    "description": "Mesial-Occlusal Facial"
   }
  },
  {
   "surface": {
    "code": "MOL",
    "description": "Mesial-Occlusal Lingual"
   }
  },
  {
```

```
  "surface": {
   "code": "MOLF",
   "description": "Mesial-Occlusal Lingual Facial"
  }
 },
 {
  "surface": {
   "code": "OL",
   "description": "Occlusal"
  }
 },
 {
  "surface": {
   "code": "OL",
   "description": "Occlusal Lingual"
  }
 }
]
```


8.0 Data Bundling by Provider Type

For the purpose of addressing the needs for each specific healthcare provider, while not overwhelming that provider with information that is extraneous to their specific care provided, data bundles are structured within this Section. As with all DSDs, data bundles within this Section shall be structured as either referenced within the FHIR Standard, the SNOMED Standard or as referenced within this document.

8.1 Dental Referral Data Bundling

Information that shall be included when a dental care provider is communicating with another provider for the purpose of endodontic, oral facial pain, oral surgical, orthodontic, pedodontic, periodontal, prosthodontic or other dental treatment includes the following information as outlined in this document:

A. The Care Provider Electronic Information
B. The patient's EHI
C. The reason for referral, including any tooth number(s)
D. Degree of urgency, with the options:
    i. Emergency/Urgent, right away
    ii. Routine, within 2 weeks if possible
    iii. Recommended, recommended to patient

Information that should be included when a dental care provider is communicating with another provider for the purpose of endodontic, oral facial pain, oral surgical, orthodontic, pedodontic, periodontal, prosthodontic or other dental treatment includes the following

information as outlined in this document:

A. Exam details including, including any tooth number(s)
B. The patient's DMHS
C. Any diagnostic testing results including vitality testing, reported pain, swelling, or sensitivity
D. History of prior dental treatment of the tooth (teeth)
E. Attachment or ability to view associated radiographs, including intraoral, panoramic or CBCT, within an accredited Standard data structure to view (examples include STL[22], DICOM[23] and JPEG[24])

8.2 Data Bundling for Healthcare Providers Not Defined Within This Section

DSD that shall be included when a dental care provider is communicating with another provider for the purpose of non-dental treatment includes the following conditions as outlined in this document:

A. The Care Provider Electronic Information
B. The patient's EHI
C. The patient's DSS
D. The patient's DMHS

9 Information Security

9.1 ODIN Authentication

Authentication is the process of determining whether someone is, in fact, who they say they are. Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access.

As professionals often access EDR's at multiple dental practices, either as part of a dental group or across multiple dental practices, and not all users are actively treating dental patients in the line of care, or handling payment processing on behalf of the patient. All Users shall be required to log into the minimal level of EDR accessibility including:

A. Corporate EDR accessibility
B. Region EDR accessibility
C. Group EDR accessibility
D. Single practice EDR accessibility
E. Business User without access to ePHI, including DSDs

Therefore, Users shall have only access to the DSDs and EDRs that are minimally necessary for their Roles. Users shall be required to use Multi-factor authentication using an authenticator app or a physical security key, as SMS-based, telephone-based, and email-based multi-factor authentication methods are not encrypted and vulnerable to phishing[a,b,c]. Therefore SMS-

based, telephone-based, and email-based multi-factor authentication methods shall not be used or deemed sufficient for authentication for ODIN systems.

9.2 Roles and Permissions to access ODIN

User permission is an authorization given to users to access specific resources and perform specific functions. User role is a predefined category that can be assigned to users on the basis of their job title or some other criteria. Once assigned, the role automatically assigns a set of one or more permissions to the user.

The ODIN system shall identify the following roles:

- Organization Admin
- Organization Care User
- Organization User
- Region Admin
- Region Care User
- Region User
- Office Admin
- Office Care User
- Office User

All Admin and Care User assignments shall be considered in the line of care, having access to ePHI where permitted given overseeing Standards (including HIPAA), whereas non-Admin and non-Care Users shall be considered not in the line of care, thereby not having accessibility to ePHI.

Special permission shall be granted to users before they can access ePHI. This may be done automatically by mapping users to their provider records or manually by Administrator assigning ePHI permission.

9.3 Encryption and Cryptography

All ePHI shall be protected through the use of strong cryptography with associated key management processes and procedures to protect the confidentiality, authenticity and/or integrity of information that then shall be documented.

Furthermore, all remaining non-ePHI information should be protected through encryption whenever reasonable through the use of strong cryptography with associated key management processes and procedures that then shall be documented.

All encryption shall be performed in accordance with industry Standards, including NIST[25].

9.3.1 Data At-Rest

Data at-rest refers to data residing in computer storage in any digital form. At-rest data encryption protects data during storage, whether on a mobile device, computer, tablet, data warehouse, or in the cloud. Data at-rest is a target for hackers because of its static data storage and logical structure.

All ePHI data shall be encrypted at-rest in accordance with industry Standards, including NIST.

Non-ePHI data should be evaluated for encryption through consideration of the nature, scope, context, and purposes of processing. Additionally, the risks and severity to the rights and freedoms of patients and clinicians should be taken into account, as well as the implementation of appropriate technical and organizational measures surrounding the pseudonymization and encryption of data to ensure a level of security appropriate to the risk in accordance with existing Standards, such as HIPAA and NIST.

9.3.2 Data In-Transit

Data in-transit refers to data in motion or while it's being transferred. Data is more vulnerable while in-transit than when at-rest, therefore this data requires additional security protocols to protect it.

All data in-transit over the Internet or local company Intranet shall be protected with the TLS[26] v1.2 protocol or better. All ePHI in-transit shall be additionally protected by authenticating the sender and receiver before decrypting the information upon arrival using Transport Layer Security (TLS).

9.4 Traffic Access Control / Request Blocking and Filtering

Traffic Access Control protects against vulnerabilities and exploits, such as SQLi or XSS attacks and filters out unwanted traffic by user's geographical location or by defining specific patterns.

The system shall implement methods of protection against cyber attacks using the following criteria:

A. IP addresses that requests originate from
B. Country or Geo location that requests originate from
C. Length of requests
D. Values in request headers
E. Values in request bodies
F. Presence of a malicious SQL[27] code (SQL injection)
G. Presence of a malicious script (cross-site scripting)

Traffic from geo locations and countries with high risks of unauthorized data access attempts should be geo-blocked.

9.5 Fraud Prevention

Account takeover is an illegal activity in which an attacker gains unauthorized access to a user's account. The attacker might pose as the victim to gain access to other victim's accounts, other user accounts in the healthcare practice, or gain access to offices' data.

When users log on/off the system, the information about their login attempts shall be recorded and retained in accordance with existing regulation, including HIPAA. Important user activity should also be captured and saved in the user activity log. The system shall periodically analyze user activity for patterns of anomalous login attempts, compromised credentials, and unauthorized user activity, and alert the office administrator on any findings.

9.6 Privacy Mode

Privacy mode keeps ePHI protected during user activity. When Privacy mode is enabled, all of the ePHI is hidden or blurred to be unreadable to users. This prevents unauthorized users from reading and divulging ePHI data.

Privacy mode shall be automatically enabled after 15 minutes of inactivity or less, as a system should not rely on users locking their session before stepping away to reduce the risk of unauthorized data access.

Users should be required to enter a password in order to disable Privacy mode after a period of inactivity.

10 API

10.1 Data Formats

The JSON[28] representation for a resource is based on the JSON format or as defined in FHIR.

The NDJSON[29] (Newline delimited JSON) is a variant of the JSON format recommended for bulk transfers.

The CSV[30] (comma-separated values) file is a delimited text file that uses a comma to separate values where each line of the file is a data record.

10.2 API Versioning

API versioning is the practice of managing changes to an API and ensuring that these changes are made without disrupting clients. A good API versioning strategy clearly communicates the changes made and allows API consumers to decide when to upgrade to the latest version at their own pace.

The system shall implement one of the following versioning methods:

A. Versioning through URI Path.
Example: api.example.com/1/products

B. Versioning through query parameters.
Example: api.example.com/products?version=1

C. Versioning through custom headers.
Example: curl -H “Accepts-version: 1.0” https://api.example.com/products

D. Versioning through content negotiation.
Example: curl -H “Accept: application/vnd.xm.device+json; version=1”
http://www.example.com/api/products

10.3 API Authentication and Authorization

With machine-to-machine (M2M) applications, the system authenticates and authorizes the app rather than a user. For this scenario, typical authentication schemes like username + password or social logins shall be deemed insufficient.

M2M applications shall use the Client Credentials Flow, in which they pass along their Client ID and Client Secret to authenticate themselves and get a token.

10.4 Reading and Sending Information

10.4.1 Direct Requests

Direct Request is a Request-Response REST API call. It is the most direct way to retrieve data or perform action. Direct requests may support complex search criteria and be throttled by limiting the number of requests made in a certain period or by the maximum number of records returned.

Read Examples:

GET https://api.example.com/1/organizations/{organizationId}/providers
GEThttps://api.example.com/1/organizations/{organizationId}/providers?firstname=JohnGET https://api.example.com/1/groups/{groupIds}/organizations
GET https://api.example.com/1/groups/{groupIds}/organizations?created=prevMonth
GET https://api.example.com/1/organizations/{organizationId}

Create Examples:

POST https://api.example.com/1/organizations/{organizationId}/patients

Update Examples:

PUT https://api.example.com/1/organizations/{organizationId}/patients/{patientId}

10.4.2 Deltas

Delta is a variant of a direct request that enables applications to discover newly created, updated, or deleted records. Deltas should accept a time period as an input parameter.

Examples:

GET
https://api.example.com/1/organizations/{organizationId}/providers?fromModifiedDate=20230101&toModifiedDate=20230131

10.4.3 Batches

Batch is a Publish-Subscribe REST API call that enables applications to request or update large chunks of data in one request. Batches do not have the same throttling constraints as Deltas and, thus, can return an unlimited number of records. The process of preparing the results is executed in the background and can take time to finish. Once the response data has been prepared, the system shall callback a webhook previously registered by the caller.

The system shall allow 2 types of Batch Requests: Setup and Incremental. Setup shall return the results of multiple Direct Requests. Incremental shall return the full Delta.

Examples:

https://api.example.com/1/organizations/{organizationId}/patients/batch/setup
https://api.example.com/1/organizations/{organizationId}/patients/batch/incremental?fromModifiedDate=20230101&toModifiedDate=20230131

10.4.4 Web Hooks

Webhooks are a way for applications to communicate with each other using ever-driven architecture. The calling application registers its own url either manually via User Interface or by calling a webhook sign-up API. Once registered, it will be notified once registered events occur.

Example:

POST https://api.example.com/1/webhook

Annex A

Non-Normative References

1. Greenberg A, So Hey You Should Stop Using Texts For Two-Factor Authentication, WIRED (2016)
2. Elliott M, Do You Use SMS For Two-Factor Authentication? Here's Why You Shouldn't, CNET (2020)
3. NIST: SMS Authentication Is Not Secure, AET Europe Online (2017)
4. Data Integrity Strategies For Patient Matching Identification, Health Analytics (2017)
5. Soloman I. Appavu, Analysis of Unique Patient Identifier Options, The Department of Health and Human Services (1997)

ADA American Dental Association®
America's leading advocate for oral health

211 East Chicago Avenue, Chicago, Illinois 60611
T 312.440.2500 F 312.440.7494 www.ada.org