Q-11011/3/2015-eGov
Government of India
Ministry of Health and Family Welfare
eHealth Section
*****

Nirman Bhawan, New Delhi
Date: 30th Dec, 2016

Circular

Subject: Notification of Electronic Health Record (EHR) Standards - 2016 for India -reg.

With an objective to introduce a uniform standard-based system for creation and maintenance of Electronic Health Records (EHRs) by the healthcare providers, Ministry of Health and Family Welfare notified EHR Standards for India in 2013.

2. With the passage of time, the EHR Standards 2013 have been duly revised in line with the contemporary developments, in consultation with the stakeholders at large.

3. Accordingly, EHR Standards 2016 document is notified and is placed herewith for adoption in IT Systems by healthcare institutions/providers across the country.

(Jitendra Arora)
Director(eHealth)
Ministry of Health & Family Welfare
Ph: 23062317

e-Health Division
Department of Health & Family Welfare
Ministry of Health & Family Welfare
Government of India
mohfw.nic.in

ELECTRONIC HEALTH RECORD (EHR) STANDARDS FOR INDIA

2016

Standards Set Recommendations v2.0

TABLE OF CONTENTS

Contents

Executive Summary

INTRODUCTION

In September 2013 the Ministry of Health & Family Welfare (MoH&FW) notified the Electronic Health Record (EHR) Standards for India. The set of standards given therein were chosen from the best available and used standards applicable to Electronic Health Records from around the world keeping in view their suitability to and applicability in India. The Committee constituted to recommend the standards drew from experts, practitioners, government officials, technologists, and industry. The notified standards were not only supported by professional bodies, regulatory bodies, stakeholders, but various technical and social commentators as well, as being a step in the right direction. MoH&FW moved ahead with facilitating the adoption, as next steps, and in last two years the Ministry has made available standards like SNOMED CT free-for-use in the country as well as appoint interim National Release Center (NRC) to handle this clinical terminology standard that is fast gaining widespread acceptance amongst the various healthcare IT stakeholder communities worldwide.

At the time of notifying the standards in September 2013, it was understood that the standards themselves will continue to evolve over time. Consequently, it was accepted that this notification will require revision from time to time. This becomes all the more necessary as understanding of those standards, their implementation and the expectations from the healthcare systems improve. Hence, MoH&FW constituted an expert group to review the earlier notified set of standards based on the experience and with eyes firmly on the future. The set of standards provided herein represents the recommendations of the Expert Committee arrived at after deliberating on the various aspects of standardizations in healthcare record systems. The Committee also carefully examined the provisions of open standards and the guidelines as per the norms suggested by MeitY, Government of India and recommended the standards given later in the document.

NEED FOR ELECTRONIC HEALTH RECORD

For a health record of an individual to be clinically meaningful it needs to be from conception or birth, at the very least. As one progresses through one's life, every record of every clinical encounter represents a health-related event in one's life. Each of these records may be insignificant or significant depending on the current problems that the person is suffering from. Thus, it becomes imperative that these records be available, longitudinally arranged as a time series, and be clinically relevant to provide a summary of the various healthcare events in the life of a person.

An Electronic Health Record (EHR) is a collection of various medical records that get generated during any clinical encounter or events. With rise of self-care and homecare devices and systems, nowadays meaningful healthcare data get generated 24x7 and also have long-term clinical relevance. The purpose of collecting medical records, as much as possible, are manifold – better and evidence based care, increasingly accurate and faster diagnosis that translates into better treatment at lower costs of care, avoid repeating unnecessary investigations, robust analytics including predictive analytics to support personalized care, improved health

EXECUTIVE SUMMARY

policy decisions based on better understanding of the underlying issues, etc., all translating into improved personal and public health.

Without standards, a lifelong medical record is simply not possible, as different records from different sources spread across ~80+ years, potentially, needs to be brought meaningfully together. To achieve this, a set of pre-defined standards for information capture, storage, retrieval, exchange, and analytics that includes images, clinical codes and data is imperative.

STRATEGIC HIGHLIGHTS

This document provides a structured overview of the key EHR standards with respect to Indian healthcare system. For every aspect of data/information that is part of any healthcare record system has been addressed with a short guideline regarding implementation specific to the item-in-context included. Various non-related recommendations from previous edition have been removed to better streamline the set of standards selected and achieve harmony among them. A detailed recommendation on the interoperability and standards, clinical informatics standards, data ownership, privacy and security aspects, and the various coding systems are also provided. The set of standards given in earlier edition has been updated with their latest versions as the country moves towards a better implementation. It would not be out of place to note that certain sections of the document have been removed to provide increased readability and consistency throughout while avoiding duplication, ambiguity and contradictions.

SCOPE

This document provides a set of recommendations relevant to adoption of electronic health informatics standards in EHR/EMR and other similar clinical information systems. The scope is limited to identifying the standards, their intended purposes in such systems, followed by a short guideline-for-implementation approach. It is understood that with adoption of these standards properly, the data capture, storage, view, presentation, and transmission will be standardized to levels that will achieve interoperability of both meaning and data contained in the records. This document does not cater to wider implementation scenarios such as of administrative, legal or regulatory nature. This document also does not cater to aspects of creation and operation of local, regional or national infrastructures, indexes, or repositories as they are dealt with by appropriate regulative/administrative bodies.

LOOKING AHEAD

This document is a continuation of its earlier version, but in many ways reflects the growing confidence in the path correctly chosen earlier – providing a set of international and proven standards with focus towards achieving syntactic and semantic interoperability of health records. The idea that any person in India can go to any health service provider/practitioner, any diagnostic center or any pharmacy and yet be able to access and have fully integrated and always available health records in an electronic format is not only empowering but also the vision for efficient 21st century healthcare delivery.

EXECUTIVE SUMMARY

In conclusion, it must be reiterated that these standards cannot be considered either in isolation or as “etched in stone for all eternity”. These will need to undergo periodic review and update as necessary. Hence, it is imperative that this document be a “living document”.

Standards at a Glance

This section is provided for quick reference. Details are provided in the subsequent sections.

N.B., this is a tentative list only.

S. No.	Type	Standard Name	Intended Purpose
1	Identification & Demographics	ISO/TS 22220:2011 Health Informatics – Identification of Subjects of Health Care	Basic identity details of patient
2		MDDS – Demographic (Person Identification and Land Region Codification) version 1.1	Complete demographic for interoperability with E-Governance systems
3	Patient Identifiers	UIDAI Aadhaar	Preferable identifier where available
4		Local Identifier	Identifier given within institution / clinic / lab
5		Government Issued Photo Identity Card Number	Identifier used in conjunction with local in absence of Aadhaar
6	Architecture Requirements	ISO 18308:2011 Health Informatics – Requirements for an Electronic Health Record Architecture	System architectural requirements
7	Functional Requirements	ISO/HL7 10781:2015 Health Informatics - HL7 Electronic Health Records-System Functional Model Release 2 (EHR FM)	System functional requirements
8	Reference Model and Composition	ISO 13940 Health informatics - System of Concepts to Support Continuity of Care	Concepts for care, actors, activities, processes, etc.
9		ISO 13606 Health informatics - Electronic Health Record Communication (Part 1 through 3)	Information model architecture and communication
10		openEHR Foundation Models Release 1.0.2	Structural definition and composition
11	Terminology	SNOMED Clinical Terms (SNOMED CT)	Primary terminology
12	Coding System	Logical Observation Identifiers Names and Codes (LOINC)	Test, measurement, observations

STANDARDS AT A GLANCE

S. No.	Type	Standard Name	Intended Purpose
13		WHO Family of International Classifications (WHO-FIC) including ICD, ICF, ICHI, ICD-O	Classification and reporting
14	Imaging	Digital Imaging and Communications in Medicine (DICOM) PS3.0-2015	Image, waveform, audio/video
15	Scanned or Captured Records	JPEG lossy (or lossless) with size and resolution not less than 1024px x 768px at 300dpi	Image capture format
16		ISO/IEC 14496 - Coding of Audio-Visual Objects	Audio/Video capture format
17		ISO 19005-2 Document Management - Electronic Document File Format for Long-Term Preservation - Part 2: Use of ISO 32000-1 (PDF/A-2)	Scanned documents format
18	Data Exchange	ANSI/HL7 V2.8.2-2015 HL7 Standard Version 2.8.2 - An Application Protocol for Electronic Data Exchange in Healthcare Environments	Event/Message exchange
19		ASTM/HL7 CCD Release 1 (basis standard ISO/HL7 27932:2009)	Summary Records exchange
20		ISO 13606-5:2010 Health informatics - Electronic Health Record Communication - Part 5: Interface Specification	EHR archetypes exchange [Also, refer to openEHR Service Model specification]
21		DICOM PS3.0-2015 (using DIMSE services & Part-10 media/files)	Imaging/Waveform Exchange
22	Other Relevant Standards	Bureau of Indian Standards and its MHD-17 Committee	Standards Development Organizations (SDOs)
23		ISO TC 215 set of standards	
24		IEEE/NEMA/CE standards for physical systems and interfaces	
25	Discharge/ Treatment Summary	Medical Council of India (MCI) under regulation 3.1 of Ethics	Composition as prescribed
26	E-Prescription	Pharmacy Practice Regulations, 2015 Notification No. 14-148/ 2012- PCI as specified by Pharmacy Council of India	Composition as prescribed
27	Personal Healthcare and medical Device Interface	IEEE 11073 health informatics standards and related ISO standards for medical devices	Device interfacing

STANDARDS AT A GLANCE

S. No.	Type	Standard Name	Intended Purpose
28	Data Privacy and Security	ISO/TS 14441:2013 Health Informatics – Security & Privacy Requirements of EHR Systems for Use in Conformity Assessment	Basis security and privacy requirements
29	Information Security Management	ISO/DIS 27799 Health informatics - Information Security Management in Health using ISO/IEC 27002	Overall information security management
30	Privilege Management and Access Control	ISO 22600:2014 Health informatics - Privilege Management and Access Control (Part 1 through 3)	Access control
31	Audit Trail and Logs	ISO 27789:2013 Health informatics - Audit trails for Electronic Health Records	Audit trail
32	Data Integrity	Secure Hash Algorithm (SHA) used must be SHA-256 or higher	Data Hashing
33	Data Encryption	Minimum 256-bits key length	Encryption key
34		HTTPS, SSL v3.0, and TLS v1.2	Encrypted connection
35	Digital Certificate	ISO 17090 Health informatics - Public Key Infrastructure (Part 1 through 5)	Digital certificates use and management

***Note**: Where year of publication or version of standard (or its parts) is not provided explicitly, the latest published version of standard (or its parts) available from standard body as on the date of notification / circulation of this recommendation is to be used.*

STANDARDS AT A GLANCE

List of Supporting / Complimenting Standards

The following list is indicative and representative and not comprehensive or definitive. These standards are advised to be used where applicable and as required.

S. No.	Standard	Description
1	ISO 12967:2009	Health Informatics - Service Architecture (Parts 1 - 3)
2	ISO 13972:2015	Health Informatics - Detailed Clinical Models, Characteristics and Processes
3	ISO 20301:2014	Health Informatics - Health Cards - General Characteristics
4	ISO 21090:2011	Health Informatics - Harmonized Data Types for Information Interchange
5	ISO 8601:2004	Data elements and Interchange Formats - Information Interchange - Representation of Dates and Times
6	ISO 13119:2012	Health Informatics - Clinical Knowledge Resources - Metadata
7	ISO 22857:2013	Health Informatics – Guidelines on Data Protection to Facilitate Trans-Border Flows of Personal Health Data
8	ISO 21549-1:2013	Health Informatics — Patient Healthcard Data — Part 1: General Structure
9	ISO TS 14265:2011	Classification of Purposes for Processing Personal Health Information
10	ISO TS 27527:2010	Health Informatics – Provider Identification

Standards and Interoperability

INTEROPERABILITY STANDARDS

The primary aim of interoperability standards is to ensure syntactic (structural) and semantic (inherent meaning) interoperability of data amongst systems at all times. The need for that cannot be overstated, more so within healthcare information systems whose primary aim is to deliver life-long clinical care at all times so that the person being cared for is able to maintain his/her health at optimal levels.

The set of standards outlined in this document represents an incremental approach to adopting standards, implementation specifications; criteria to enhance the interoperability, functionality, utility, and security of health information technology; and to support its widespread adoption. It is to be kept in mind that these standards need to be flexible and modifiable to adapt to the demographic and resource variance observed in a country like India with its large population and diverse culture that is spread across a large region of varied geographical landscapes – hilly regions, river basins, desert, coast, etc. – many of which are remote and accessible only with difficulty.

It is important to recognize that interoperability and standardization can occur at many different levels. To achieve interoperability, information models would need to be harmonized into a consistent representation.

In other cases, organizations may use the same information model, but use different vocabularies or code sets (for example, SNOMED CT or ICD10) within those information models. To achieve interoperability at this level, standardizing vocabularies, or mapping between different vocabularies may be necessary. For some levels, (such as the network transport protocol), an industry standard that is widely used (e.g. TCP/IP – Transmission Control Protocol and Internet Protocol) will likely be the most appropriate. Ultimately, to achieve true interoperability, it is anticipated that multiple layers – network transportation protocols, data and services descriptions, information models, and vocabularies and code sets – will need to be standardized and/or harmonized to produce an inclusive, consistent representation of the interoperability requirements.

It is further anticipated that using a harmonization process will integrate different representations of health care information into a consistent representation and maintain and update that consistent representation over time. For an information model, this process could include merging related concepts, adding new concepts, and mapping concepts from one representation of health care information to another. The need to support standardization of data and services descriptions and vocabularies and codes sets is appropriately addressed.

It is also recognized that a sustainable and incremental approach to the adoption of standards will require processes for harmonizing both current and future standards. This will allow the incremental updating of the initial set of standards, implementation specifications, and certification criteria and provide a framework to maintain them. The decision to adopt such updates will be informed and guided by recommendations from an appropriate authority such as the proposed National eHealth Authority (NeHA), Ministry of Health & Family Welfare or expert groups.

STANDARDS AND INTEROPERABILITY

GOALS

The goals of standards in electronic health record systems are:

- Promote interoperability and where necessary be specific about certain content exchange and vocabulary standards to establish a path forward toward semantic interoperability
- Support the evolution and timely maintenance of adopted standards
- Promote technical innovation using adopted standards
- Encourage participation and adoption by all vendors and stakeholders
- Keep implementation costs as low as reasonably possible
- Consider best practices, experiences, policies and frameworks
- To the extent possible, adopt standards that are modular and not interdependent.

Health Record IT Standards

IDENTIFICATION AND DEMOGRAPHIC INFORMATION OF PATIENT

Demographic information including a unique identifier is necessary in a health record system in order to capture identifying information as well as identifiers for linking other medical artifacts logically as well as physically. All health record systems must therefore adhere to the following standards for capturing information related to patient demography and identifiers:

1. ISO/TS 22220:2011 Health Informatics – Identification of Subjects of Health Care
2. MDDS – Demographic (Person Identification and Land Region Codification) version 1.1 from E-Governance Standards, Government of India

Implementation Guideline: Implementers must insure that health record application is able to capture all data fields as provided in the above two standards for completeness. It should also ensure that the system is able to interoperate (receive/import/send/export) all demographics information as provided in above two standards as per demand, i.e. when requested for demographics data in MDDS compliant format it should generate artefacts (file, message, etc.) as per that standard. Where codes related to location, authority, type of organization etc. are required, they should be taken from the MDDS-Demographic Standard.

A health record system must have provision to include patient identifiers of following types:

1. UIDAI Aadhaar Number (preferred where available)
2. Both of the following in case Aadhaar is not available:

   2.1 Local Identifier (as per scheme used by HSP)

   2.2 Any Central or State Government issued Photo Identity Card Number

Implementation Guidelines:

1. Implementers must ensure that the Aadhaar number, where that is available, be used as the preferred identifier to serve as the unique health identifier. In case the Aadhaar number is not available, the system should allow a user to insert more than one (minimum of two) identifiers for each patient along with its scope and provider (as given in above mentioned patient demography standards) in the system. In situations where identity of patient cannot be obtained or ascertained, temporary identifiers may be used (as per scheme used by HSP) and later confirmed identifiers may be inserted (while making earlier ones as inactive).
2. *Identification of Patient across EHR systems*: Due to lack of mandate for use of Aadhaar or any such alternative(s) national unique identifier, it is difficult to match patient records when exchanging them between two EHR systems. This may lead to situations where different combinations of local identifier and photo identity card numbers of the same person are used at different locations and/or in solutions.

Thus, a single person may get to have different identities under which his/her records are captured. A conflict resolution process may be required to help resolve such cases. At this time, there is no direct solution available other than to use smart (possibly heuristic) algorithms to attempt to match records without or with intervention/confirmation of a human supervisor. Such an algorithm may use name (phonetic or spelling), address (full or parts), date of birth / age, gender, or other such matching details to mark incoming or searched records as possible or exact match before amalgamation or subsequent use. ISV may additionally need to provide the ability to merge/demerge patients to support this process within their solutions.

ARCHITECTURE REQUIREMENTS AND FUNCTIONAL SPECIFICATIONS

A health record system must meet architectural requirements and functional specifications to remain faithful to the needs of service delivery, be clinically valid and reliable, meet legal and ethical requirements, and support good medical practices. Therefore, a health record system must conform to the following standards:

1. ISO 18308:2011 Health Informatics – Requirements for an Electronic Health Record Architecture
2. ISO/HL7 10781:2015 Health Informatics - HL7 Electronic Health Records-System Functional Model Release 2 (EHR FM)

Implementation Guideline: Above two standards, despite being extensive, do not represent the full set of specifications and requirements that need to be met by a health record system or its many variants (PHR, etc.) or all possible use cases. The above mentioned standards are to be used as minimum set to be used within the scope of implementation as per relevance to the system being developed / deployed.

LOGICAL INFORMATION REFERENCE MODEL AND STRUCTURAL COMPOSITION

A health record system must accumulate observable data and information for all clinically relevant events and encounters. For this purpose, it is important to have common semantic and syntactic logical information model and structural composition for captured artefacts. Unless the data being captured is standardized, its communication and understanding may not be same across systems. Therefore, a health record system must conform to the following standards:

1. ISO 13940 Health Informatics - System of Concepts to Support Continuity of Care
2. ISO 13606 Health Informatics - Electronic Health Record Communication (Part 1 through 3)
3. openEHR Foundation Models Release 1.0.2

   3.1 Required Model Specifications: Base Model, Reference Model, Archetype Model

   3.2 Optional Model Specifications: Service Model, Querying, Clinical Decision Support

Implementation Guideline: The ISO 13940 (also known as CEN ContSys) is to be generally used for purpose of modelling and describing concept system and organize information objects. While ISO 13606 set of standards are basic reference model and related specifications, openEHR provides ISO 18308 conformant

platform-independent implementation harmonized with ISO 13606 standard. Implementers are free to design internal structures, databases, and user interfaces as per their requirements and preferred technology platforms but structural composition for clinical data/information artefact must be logically similar to Reference Model given in above standards. openEHR Operational Templates (OPT) adopted by an implementation, are to be public and free in required format for other implementers to ensure interoperability among them.

MEDICAL TERMINOLOGY AND CODING STANDARDS

In order to have semantic interoperability between different health record systems, it is necessary to follow a common terminology and coding system standards to express unambiguous meaning of data captured, stored, transmitted, and analyzed. It is also important to have these terminologies and codes in computer process-able format to aid automation and ensure that data is in an analyzable state at all times. Therefore, a health record system must conform to the following standards:

1. Primary Terminology: IHTSDO - SNOMED Clinical Terms (SNOMED CT)

Implementation Guideline: A health record system must use SNOMED CT as the primary internal encoding system for all clinically relevant, including dental, nursing, substance/drugs related information. IHTSDO SNOMED CT code shall also be used while communicating clinical information to other health record systems. SNOMED CT concept codes (as pre-coordinated or as post-coordinated expressions) are to be used for all hierarchies covered under the standard unless otherwise provided in this document. It shall also be the coding system that must be used internally in other information storage and communication standards such as openEHR archetypes, HL7, DICOM, etc. IHTSDO releases SNOMED CT twice annually.

2. Test, Measurement and Observation Codes: Regenstrief Institute - Logical Observation Identifiers Names and Codes (LOINC)

Implementation Guideline: LOINC coding is to be used for processing results and reports with Laboratory and Imaging Information Systems. N.B.: SNOMED CT to LOINC coding interchange map is available from IHTSDO and Regenstrief Institute.

3. Classification Codes: WHO Family of International Classifications (WHO-FIC)

    3.1 WHO ICD-10: International Classification of Diseases (ICD) and its derivative classifications

    3.2 WHO ICF: International Classification of Functioning, Disability and Health (ICF)

    3.3 International Classification of Health Interventions (ICHI)

    3.4 International Classification of Diseases for Oncology (ICD-O)

Implementation Guideline: WHO FIC codes are primarily used for aggregated information and statistical/epidemiological analysis for public health purposes derived from health records that contain patient care related information as well as information that is crucial for management, health financing and

general health system administration. While SNOMED CT is to be used by health record systems for terminology, generated classification-based reports may require the use of WHO FIC codes. Classification based reporting, for statistical or regulatory purposes, may continue to use WHO FIC codes as mandated by the health regulatory, intelligence, and various research bodies. N.B.: SNOMED CT to ICD-10 coding interchange map is available from IHTSDO and WHO.

DATA STANDARDS FOR IMAGE, MULTIMEDIA, WAVEFORM, DOCUMENT

A health record system stores data records and files of various types in support of clinical functions. These data elements serve the purpose of documentary records of various diagnostic and prescriptive data or information generated. Therefore, a health record system must conform to the following standards for such data:

1. NEMA Digital Imaging and Communications in Medicine (DICOM) PS3.0-2015

Implementation Guideline: NEMA DICOM PS3.0-2015 is a comprehensive standard for handling and managing image (series or single), waveforms (such as those in ECG/EEG), audio (such as those in digital-stethoscope) and video (such as those in endoscope, ultrasound, etc.) data in medicine. A health record implementation is required to implement relevant DICOM Information Object Definitions (IODs) for supported data types in Part-10 compliant files. Where required and relevant, other features of standard such as services, display, print, and workflow may be implemented.

2. Scanned or Captured Records:

    2.1 Image: JPEG lossy (or lossless) with size and resolution not less than 1024px x 768px at 300dpi

    2.2 Audio/Video: ISO/IEC 14496 - Coding of Audio-Visual Objects

    2.3 Scanned Documents: ISO 19005-2 Document Management - Electronic Document File Format for Long-Term Preservation - Part 2: Use of ISO 32000-1 (PDF/A-2) (ref: Best Practices and Guidelines for Production of Preservable e-Records Ver1.0 from MeitY, Govt. of India)

Implementation Guideline: The above mentioned standards are to be used for documentary data (scan for prescription, summaries, etc.) and data captured through traditionally non-DICOM compliant sources like picto-micrographs, pathological photographs, photographs of intramural and extramural lesions, etc. All data formats that can be converted into relevant DICOM format should be, as relevant, converted and communicated as secondary captured DICOM format. It may be noted that while no maximum image resolution has been prescribed, a sufficiently acceptable limit may be used to avoid unnecessarily large file that do not aid in correspondingly better interpretation or analysis.

DATA EXCHANGE STANDARDS

A health record system has to operate in a larger ecosystem of other components with which it must share or communicate data in order to capture and provide as comprehensible medical information as is practical. A health record system must therefore conform to the following standards:

1. Event/Message Exchange: ANSI/HL7 V2.8.2-2015 HL7 Standard Version 2.8.2 - An Application Protocol for Electronic Data Exchange in Healthcare Environments
2. Summary Records Exchange: ASTM/HL7 CCD Release 1 (basis standard ISO/HL7 27932:2009)
3. EHR Archetypes: ISO 13606-5:2010 Health informatics - Electronic Health Record Communication - Part 5: Interface Specification [Also, refer to openEHR Service Model specification]
4. Imaging/Waveform Exchange: NEMA DICOM PS3.0-2015 (using DIMSE services& Part-10 media/files)

Implementation Guideline: Implementation of exchange standards is expected to be at least for the scope of data captured or retained by the health record system. To explain further, full implementation of ANSI/HL7 V2.8.2 for each event and message is not required in health record systems but minimum implementation supporting the types of events and messages relevant to the system is required. Similarly, implementation/support of DICOM DIMSE C-Store and/or C-FIND/C-GET service is expected for IODs supported by health record system whereas implementation of WADO could be optional.

OTHER STANDARDS RELEVANT TO HEALTHCARE SYSTEMS

Healthcare record systems need to co-exist within a larger ecosystem with various other systems. It is important for all systems within a healthcare setup to adhere to relevant standards. While standards related to such systems are not within the scope of this document, as a general rule, standards created or ratified by following Standard Development Organizations (SDOs) should be used:

1. Bureau of Indian Standards and its MHD-17 Committee
2. ISO TC 215 set of standards
3. IEEE/NEMA/CE standards for physical systems and interfaces

Implementation Guideline: To help the implementers, an indicative list of such standards is provided in the "Standards at a Glance" section above. Wherever applicable, BIS-approved standards shall be preferred for implementation.

DISCHARGE/TREATMENT SUMMARY FORMAT

Implementers must ensure that the logical information model includes data elements to satisfy requirements of the format for Medical Records as specified by Appendix-3 of Medical Council of India (MCI) Code of Ethics Regulation 2002 (amended up to Feb-2016). The printed reports should meet MCI prescribed formats whenever any discharge or treatment summary is prepared.

E-PRESCRIPTION

Pharmacy Council of India (PCI) has, in its recent regulation (Pharmacy Practice Regulations, 2015 Notification No. 14-148/ 2012- PCI), provided the definition of the term under Section 2(j) that the term 'Prescription' includes the term 'electronic direction'. Implementers must therefore ensure that the logical

information model includes data elements to satisfy requirements of the format for Medical Prescription as specified by the Pharmacy Council of India. The printed prescription will need to be in the PCI prescribed format whenever any medical prescription meant for drug dispensing is prepared. For the purpose of e-Prescription, implementers must ensure that the electronic version is digitally signed by a registered medical practitioner, and its non-repudiation is ensured at all times. The pharmacists shall be able to print a copy of e-Prescription in the required format along with other relevant digital authentication details.

PERSONAL HEALTHCARE AND MEDICAL DEVICES INTERFACING

Where not covered under relevant data exchange standards, it is recommended that IEEE 11073 health informatics standards and related ISO standards for medical devices be followed as appropriate whenever any personal healthcare/medical device is interfaced with the EMR system for the purpose of clinical data exchange, retrieval, storage, etc.

PRINCIPLES OF DATA CHANGE

The data once entered into a health record system must become immutable. The healthcare provider may have the option to re-insert/append any record in relation to the medical care of the patient as necessary with a complete audit trail of such change maintained by the system. Alteration of the previously saved data is not permitted. No *update* or *update like* command shall be accessible to user or administrator to store a medical record or part thereof. Any record requiring revision should create a new medical record containing the changed/appended/modified data of earlier record. This record shall then be stored and marked as ACTIVE while rendering the previous version(s) of the same record being marked INACTIVE. The data will thus in essence become immutable. A strict audit trail shall be maintained of all activities at all times that may be reviewed by an appropriate authority like auditor, legal representatives of the patient, the patient, healthcare provider, privacy officer, court appointed/authorized person, etc. as deemed necessary.

As-Is Principal:

The data captured through the devices is usually in a certain format whereas the data provided by the doctor as file may be in some different format. These data provided / included in the system are to be treated as sacrosanct. The “As-Is Principal” requires that the data captured in the first instance should be retrievable at any given point of time later in the same format, clarity, size and detail as it was provided during the time of record creation.

It effectively means that the system is not allowed to make any changes either to the data or its format or its nature at any point other than the creation time for any reason. However, if it is required that the data needs to be altered either to carry some additional information at some later point, like annotation on images, or correction of errors of omission or commission, etc., it must be done on a copy of the original data, keeping the original data intact, and marking the updated version as active while marking the previous version inactive. The modified data will then become part of the EHR/EMR.

Informed Format Change:

Whenever, the data, its format or its nature needs to be changed within the system, it must be done with the explicit consent of the doctor / technician / person that is entering or managing the data. This explicit consent can also be taken from a set of preferences already set by the user or the administrator / root of the system. In such preference based consent, there is no need to prompt the user for permission at each insertion point.

Also, in case the system is set to change format or nature of data automatically by setting of preferences, it must be made sure that the rule of conversion is declared in the Standard Operating Procedure (SOP) of site/application.

Guidelines

HARDWARE

- The IT hardware used should meet (and preferably be better than) the optimal requirements specified by the software (to be) used.
- The medical and IT hardware used must meet the relevant applicable specifications from BIS, NEMA, IEEE, ISO, CE, RoHS, EnergyStar, apart from Medical and IT standards for the equipment.
- A backup or data preservation mechanism should be put in place. Data capacity should be planned to meet the storage requirement as per the mandated rules / laws.
- System redundancy at various levels (disk, power, network, etc.) should be planned to meet the organizational system availability requirement.
- Network and data security should be planned, implemented, and periodically audited. *Please see section on Security and Privacy for the various requirements and functions that need to be supported and implemented*.
- Hardware should be checked periodically for correctness and completeness of operation expected from them. An appropriate maintenance cycle should be planned and rigorously followed.
- Planned and expected Capacity and Quality requirement of the organization should be met by the hardware used. Periodic updates and upgrades should be carried out to meet these requirements.

NETWORKING AND CONNECTIVITY

- Should be able to harness any telecommunications-related connectivity like the Internet, LAN, WAN, WAP, CDMA, GSM or even Cloud Computing that will permit the various EMRs of an individual to be integrated into a single lifelong electronic health record
- As far as is practical and affordable, the connectivity medium chosen should be reliable and fast enough to sustain a secure data exchange for the period expected for transaction of records and data. The speed of the connectivity medium should be chosen from among available options so as to provide an acceptable user experience and not cause software/system fault due to delays/noise/failure.
- Should be able to ensure that data exchange is performed in a secure manner to ensure data validity and non-repudiability
- The data exchange must further ensure that data integrity is maintained at all times

SOFTWARE STANDARDS

The software for capturing, storing, retrieving, viewing, and analyzing healthcare records should:

- Conform to the specified standards
- Satisfy specified requirements
- Be Interoperable, especially in terms of syntax and semantics of the information being exchanged

- Should be able to ensure user authentication and authorization
- Should be able to support privacy, secrecy and audit trail
- Possess advanced search, merge, and demerge functionality to ensure that duplicates are robustly resolved
- Should be able to support conception-to-current/most recent medical records of a person (as relevant to scope of application)
- Should be able to support digital archiving and retrieval of medical records after the death of a person for the total duration as specified by Government of India from time to time
- Should be able to construct a medical/clinical summary based on available records from the very first visit to current/most recent
- Preferably be able to support rapid data capture-storage-retrieval-display of data

HEALTH RECORD IN MOBILE DEVICES

As people become more mobile and travel becomes more accessible, patients will increasingly expect the healthcare record system to provide essential health information over mobile devices, which will give their treating clinician basic information like, medical condition, drug/allergy information etc. Demographics, insurance info, medications, allergy and alerts, and vital signs are some of the records that are recommended to be provided in at least read-only manner and to the extent relevant for emergency care and quick reference. It is also possible that certain clinical (BP, temperature, glucose count) and lifestyle (steps walked, distance run, sleep duration and quality) related information will additionally be provided by the patient thereby providing vital clues and information on the overall wellbeing of patient.

In the specific regard of design and usability of such applications, “Framework for Mobile Governance 2012” of DeitY, Ministry of Communication & Information Technology, Government of India shall be applicable.

Data Ownership of Health Records

THE ETHICAL, LEGAL, SOCIAL ISSUES (ELSI) GUIDELINES

For the purposes of these recommendations, the term "privacy" shall mean that only those person or person(s) including organizations duly authorized by the patient may view the recorded data or part thereof. The term "security" shall mean that all recorded personally identifiable data will at all times be protected from any unauthorized access, particularly during transport (e.g. from healthcare provider to provider, healthcare provider to patient, etc.). The term "trust" shall mean that person, persons or organizations (doctors, hospitals, and patients) are those who they claim they are.

The following approaches are to be adopted wherever applicable to address the aspects that the terms mentioned above refer to:

- Privacy would refer to authorization by the owner of the data (the patient)
- Security would have as components both public and private key encryption; the encryption techniques used in transit and at rest need to be through different methodologies.
- Trust would be accepted whenever a trusted third party confirms identity

PROTECTED HEALTH INFORMATION

Protected Health Information (PHI) would refer to any individually identifiable information whether oral or recorded in any form or medium that (1) is created, or received by a stakeholder; and (2) relates to past, present, or future physical or mental health conditions of an individual; the provision of health care to the individual; or past, present, or future payment for health care to an individual.

Electronic Protected Health Information (ePHI) would refer to any protected health information (PHI) that is created, stored, transmitted, or received electronically. Electronic protected health information includes any medium used to store, transmit, or receive PHI electronically.

As per the Information Technology Act 2000, Data Privacy Rules, refers to 'sensitive personal data or information' (SPI) as the subject of protection, but also refers, with respect to certain obligations, to 'personal information' (PI). Sensitive personal information is defined as a subset of personal information. Followings are Sensitive personal information that relates to:

1. Passwords
2. Financial information such as bank account or credit card or debit card or other payment instrument details
3. Physical, psychological and mental health condition
4. Sexual orientation
5. Medical records and history
6. Biometric information

7. Any detail relating to (1) – (6) above received by the body corporate for provision of services
8. Any information relating to (1) – (7) that is received, stored or processed by the body corporate under a lawful contract or otherwise

DATA OWNERSHIP

- The physical or electronic records, which are generated by the healthcare provider, are held in trust by them on behalf of the patient
- The contained data in record which are the protected health information of the patient is owned by the patient himself / herself.
- The medium of storage or transmission of such electronic medical record will be owned by the healthcare provider.
- The "sensitive personal information (SPI) and personal information (PI)" of the patient is owned by the patient herself. Refer to IT Act 2000 for the definition of SPI and PI.

DATA ACCESS AND CONFIDENTIALITY

- Regulations are to be enforced to ensure confidentiality of the recorded patient/medical data and the patient should have a control over this.
- Patients will have the sufficient privileges to inspect and view their medical records without any time limit. Patient's privileges to amend data shall be limited to correction of errors in the recorded patient/medical details. This shall need to be performed through a recorded request made to the healthcare provider within a period of 30 days from the date of discharge in all inpatient care settings or 30 days from the date of clinical encounter in outpatient care settings. An audit of all such changes shall be strictly maintained. Both the request and audit trail records shall be maintained within the system.
- Patients will have the privileges to restrict access to and disclosure of individually identifiable health information and need to provide explicit consent, which will be audited, to allow access and/or disclosures.
- All recorded data will be available to care providers on an 'as required on demand' basis

DISCLOSURE OF PROTECTED / SENSITIVE INFORMATION

- For use in treatment, payments and other healthcare operations: In all such cases, a general consent must be taken from the patient or next of kin, etc. as defined by the MCI.
- Fair use for non-routine and most non-health care purposes: A specific consent must be taken from the patient; format as defined by MCI.
- For certain specified national priority activities, including notifiable/communicable diseases, the health information may be disclosed to appropriate authority as mandated by law without the patient's prior authorization
- Instances where use and disclosure without individual authorization will be possible are as follows:

- Complete record with all identifiers in an "as-is" state, on production of court order
- Totally anonymized data, where the anonymization process involves the complete removal of all information that allows the identification of the patient. (List of such personally identifiable information is provided below)

RESPONSIBILITIES OF A HEALTHCARE PROVIDER

- Protect and secure the stored health information, as per the guidelines specified in this document
- While providing patient information, remove patient identifying information (as provided in the list below), if it is not necessary to be provided
- Will ensure that there are appropriate means of informing the patient of policies relating to her/his rights to health record privacy
- Document all its privacy policies and ensure that they are implemented and followed. This will include:
  - Develop internal privacy policies
  - Ensure implementation of privacy policies, audit and quality assurance
  - Provide privacy training to all its staff

PRIVILEGES OF PATIENT OR PERSONAL REPRESENTATIVE

Patient will have the privilege to carry out the activities detailed below, personally, or through their appointed representative.

- Patients can demand from a healthcare provider a copy of their medical records held by that healthcare provider, which should be provided within 30 days of receipt of communication of request.
- Patients can demand from a healthcare provider that stores/maintains his/her medical records, to withhold, temporarily or permanently, specific information that he/she does not want disclosed to other organizations or individuals.
- Patient can demand information from a healthcare provider on the details of disclosures performed on the patient's medical records for any reason whatsoever. When demanded, following details are to be provided for each instance of disclosure:
  - Date of the disclosure
  - Name and address of the entity or person who received the information
  - Brief description of the medical information disclosed
  - Brief summary of the purpose of the disclosure

DENIAL OF INFORMATION

Healthcare provider will be able to deny information to a patient or representative or third party, in contravention of normal regulations, if in the opinion of a licensed healthcare professional the release of information would endanger the life or safety of the patients and others. This will include but not be limited to as follows:

- Information obtained from an anonymous source under a promise of confidentiality.
- Psychotherapy notes.
- Information compiled for civil, criminal or administrative action.

ELECTRONIC MEDICAL RECORDS PRESERVATION

Preservation of medical records assume significant importance in view of the fact that an electronic health record of a person is an aggregation of all electronic medical records of the person from the very first entry to the most recent one. Hence, all records must compulsorily be preserved and not destroyed during the life-time of the person, ever.

Upon the demise of the patient where there are no court cases pending, the records can be removed from active status and turned to inactive status. HSPs are free to decide when to make a record inactive, however, it is preferable to follow the “three (3) year rule” where all records of a deceased are made inactive three (3) years after death.

It is however preferred, and the HSPs are strongly encouraged to ensure, that the records are never be destroyed or removed permanently. The health of the blood relatives and natural descendants of the person can be strongly influenced by the health of the person and on-demand access to these may prove to be hugely useful in the maintenance of the health of the relations.

Furthermore, analysis of health data of all persons is expected to greatly benefit in the understanding of health, disease processes and the amelioration thereof.

With rapid decline in costs of data archiving coupled with the ability to store increasing amounts of data that may be readily accessible, continued maintenance of such data is not expected to lead to any major impact on the overall system maintenance and use.

PATIENT IDENTIFYING INFORMATION

Data are "individually identifiable" if they include any of the under mentioned identifiers for an individual or for the individual's employer or family member, or if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual. These identifiers are as follows:

- Name
- Address (all geographic subdivisions smaller than street address, and PIN code)
- All elements (except years) of dates related to an individual (including date of birth, date of death, etc.)
- Telephone, cell (mobile) phone and/or Fax numbers
- Email address
- Bank Account and/or Credit Card Number
- Medical record number
- Health plan beneficiary number

- Certificate/license number
- Any vehicle or other any other device identifier or serial numbers
- PAN number
- Passport number
- AADHAAR card
- Voter ID card
- Fingerprints/Biometrics
- Voice recordings that are non-clinical in nature
- Photographic images and that possibly can individually identify the person
- Any other unique identifying number, characteristic, or code

APPLICABLE LEGISLATION

The existing Indian laws including IT Act 2000 and their amendments from time to time would prevail. (http://deity.gov.in/content/information-technology-act-2000).

Data Privacy and Security

SECURITY OF ELECTRONIC HEALTH INFORMATION:

The Privacy Standards and the Security Standards are necessarily linked. Any health record system requires safeguards to ensure that the data is available when needed and that the information is not used, disclosed, accessed, altered, or deleted inappropriately while being stored or retrieved or transmitted. The Security Standards work together with the Privacy Standards to establish appropriate controls and protections. Health sector entities that are required to comply with the Privacy Standards must also comply with the Security Standards.

Organizations must consider several factors when adopting security measures. How a healthcare provider satisfies the security requirements and which technology it decides to use are business decisions left to the individual organizations. In deciding what security measures to adopt, an organization must consider its size, complexity, and capabilities; it's technical infrastructure, hardware, and software security capabilities; the cost of particular security measures; and the probability and degree of the potential risks to the ePHI it stores, retrieves and transmits.

PURPOSE OF THE SECURITY STANDARDS

The security standards require healthcare providers to implement reasonable and appropriate *administrative*, *physical*, and *technical* safeguards to:

- ensure the confidentiality, integrity, and availability of all the e-PHI they create, transmit, receive, or maintain
- protect against reasonably anticipated threats or hazards to the security or integrity of their e-PHI
- protect against uses or disclosures of the e-PHI that are not required or permitted under the Privacy Standards
- ensure their workforce will comply with their security policies and procedures

SECURUTY TECHNICAL STANDARDS

To protect the ePHI handles by a healthcare provider, the provider must implement technical safeguards as part of its security plan. Technical safeguards refer to using technology to protect ePHI by controlling access to it. Therefore, they must address the following standards, focusing on the functionalities thereof. It is worth noting that they will need to use an EHR/EMR solution that is able to successfully and robustly demonstrate the possession and working of these functionalities.

The basic requirements for security and privacy are provided in following standard:

1. ISO/TS 14441:2013 Health Informatics – Security & Privacy Requirements of EHR Systems for Use in Conformity Assessment

Authentication:

- Locally within the system the fact that a person or entity seeking access to electronic health information is indeed the one as claimed and is also authorized to access such information must be verifiable.
- Across the network, however extensive it might be, the fact that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in this document must be verifiable.

Automatic log-off: An electronic session after a predetermined time of inactivity must be forcibly terminated. To log in back, the user will have to initiate a new log in session. However, for the sake of ergonomics, it is recommended that the unsaved state of the system at the time of automatic log-off be saved and presented back to the user for further action. This should be a user-specific feature.

The advisory standard for overall information security management in health is:

2. ISO 27799 Health informatics - Information Security Management in Health using ISO/IEC 27002

Implementation Guideline: The ISO 27799 is provided as a basic advisory standard for security management. Other security management and standard / practices / guidelines given by Law (such as IT Act 2000 and amendments) or regulatory / statutory / certification bodies (such as National Accreditation Board for Hospitals & Health care Providers (NABH)) should be taken in consideration when designing and/or implementing health record system.

Access control: The solution must assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information. In cases of emergency where access controls need to be suspended in order to save a life, authorized users (who are authorized for emergency situations) will be permitted to have unfettered access electronic health information for the duration of the emergency with the access remaining in force during the validity of the emergency situation.

Access Privileges: Ideally only clinical care providers should have access rights to a person's clinical records. However, different institutional care providers have widely varying access privileges specified that are institution-specific. No country-wide standards can be specified for this at least at this point in time.

For privilege management and access control, following standards may be used:

3. ISO 22600:2014 Health informatics - Privilege Management and Access Control (Part 1 through 3)

Implementation Guideline: The ISO 22600 set of standards is provided as an advisory standard for policy based access control. For the purpose of privilege management, rule / policy based access is expected to give better control and flexibility in defining and enforcing access control. Access control mechanisms such as Role Based, Policy Based, or singular user (applicable in case of mobile based PHR) are acceptable as long as

conformant to applicable data security law(s) and rules as well as policy of the organization where implemented.

Audit log:

- All actions related to electronic health information in accordance with the standard specified in this document including viewing should be recorded.
- All actions based on user-defined events must be recorded.
- All or a specified set of recorded audit information, upon request or at a set period of time, must be electronically displayed or printed for user/administrative review.
- All actions related to electronic health information must be recorded with the date, time, record identification, and user identification whenever any electronic health information is created, modified (non-clinical data only), deleted (stale and non-clinical data only), or printed; and an indication of which action(s) took place must also be recorded.
- A cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails should be preferably used within the system.

The advisory standard for audit trail / log in health record system is:

4. ISO 27789:2013 Health informatics - Audit Trails for Electronic Health Records

Integrity:

- During data transit the fact that the electronic health information has not been altered in transit in accordance with the standard specified in this document must be verifiable.
- Detection of events – all alterations and deletions of electronic health information and audit logs, in accordance with the standard specified in this document must be detected.
- Appropriate verification that electronic health information has not been altered in transit shall be possible at any point in time. A secure hashing algorithm must be used to verify that electronic health information has not been altered in transit and it is recommended that the Secure Hash Algorithm (SHA) used must be SHA-256 or higher.

Encryption:

- Generally, all electronic health information must be encrypted and decrypted as necessary according to organization defined preferences in accordance with the best available encryption key strength (minimum 256-bits key).

- During data exchange all electronic health information must be suitably encrypted and decrypted when exchanged in accordance with an encrypted and integrity protected link.
- Secure Transmission standards and mechanisms must be used to allow access to health information as well as transmit data from one application / site to another. For this purpose HTTPS, SSL v3.0, and TLS v1.2 standards should be used. Please refer to relevant IETF, IEEE, ISO, and FIPS standards for same.

Digital Certificates:

Use of Digital Certificates for identification and digital signing is recommended in health record system. Health record system must use following standard where digital certificates are used:

5. ISO 17090 Health informatics - Public Key Infrastructure (Part 1 through 5)

ADMINISTRATIVE SAFEGUARDS STANDARDS

The Administrative Safeguards require healthcare providers to develop and implement a security management process that includes policies and procedures that address the full range of their security vulnerabilities. Being administrative in nature, these need to be internally designed and developed as standard operating procedure (SOP) that must be published for all users to see and adhere to. Conformance to adherence may be delegated to the Privacy Officer detailed in the Data Ownership chapter above. To comply with the Administrative Safeguards, a healthcare provider must implement the following standards.

- The security management process standard, to prevent security violations;
- Assigned security responsibility, to identify a security officer;
- Workforce security, to determine e-PHI user access privileges;
- Information access management, to authorize access to e-PHI;
- Security awareness training, to train staff members in security awareness;
- Security incident procedures, to handle security incidents;
- Contingency plan, to protect e-PHI during an unexpected event; and
- Evaluation, to evaluate an organization's security safeguards.

PHYSICAL SAFEGUARDS STANDARDS

Physical safeguards are security measures to protect a healthcare provider's electronic information systems, related equipment, and the buildings housing the systems from natural and environmental hazards, and unauthorized intrusion. Healthcare providers must fulfill the following standards. However, since most of the implementation specifications in this category are addressable, healthcare providers have the flexibility in determining how to comply with the requirements as long as these are internally designed and developed as per the relevant SOP and published for all users to see and adhere to. Conformance to adherence may be delegated to the Privacy Officer detailed in the Data Ownership chapter above.

The required physical standards are:

- The facility access control standard, to limit actual physical access to electronic information systems and the facilities where they're located;
- The workstation use standard, to control the physical attributes of a specific workstation or group of workstations, to maximize security;
- The workstation security standard, to implement physical safeguards to deter the unauthorized access of a workstation; and
- The device and media controls standard, to control the movement of any electronic media containing ePHI from, to or within the facility.

Glossary

The various terms, including acronyms, are explained from a conceptual point and may not be the formal definitions.

ADSL (Asymmetric Digital Subscriber Line): A type of DSL that uses copper telephone lines to transmit data faster than a traditional modem. ADSL only works within short distances because it uses high frequencies with short signals.

Allergy List: This is a list of all the patient's allergies.

Allopathic, Allopathy: Defined as relating to or being a system of medicine that aims to combat disease by using remedies (as drugs or surgery) which produce effects that are different from or incompatible with those of the disease being treated

Ambulatory care: Any medical care delivered on an outpatient basis.

ANM: Auxiliary Nurse Midwife

Archetype: Basically an information model, it is a computable expression of a domain content model in the form of structured constraint statements, based on a reference (information) model. Within the openEHR paradigm, archetypes are based on the openEHR reference model. Archetypes are all expressed in the same formalism. In general, they are defined for wide re-use, however, they can be specialized to include local particularities. They can accommodate any number of natural languages and terminologies.

Artefact: An object made by a human being, typically one of cultural or historical interest. In healthcare IT context, an artefact is any item such as a document, file or drawing, etc. that is generated for use as a reference material or inside a system.

ASHA: Accredited Social Health Activist is usually a literate 25 – 45 year old married/ widowed/ divorced lady selected from the village itself and accountable to it and trained to work as an interface between the community and the public health system. This is position is one of the key components of the National Rural Health Mission aimed at providing every village in the country with a trained female community health activist

ATC: Anatomical Therapeutic Chemical Classification System, controlled by the WHO Collaborating Centre for Drug Statistics Methodology (WHOCC), is used for drug classification.

Authentication: The verification of the identity of a person or process.

Authorization: Any document designating any permission. Authorization or waiver of authorization for the use or disclosure of identifiable health information for research (among other activities) is required. The authorization must indicate if the health information used or disclosed is existing information and/or new information that will be created. The authorization form may be combined with the informed consent form, so that a patient need sign only one form. An authorization must include the following specific elements: a

description of what information will be used and disclosed and for what purposes; a description of any information that will not be disclosed, if applicable; a list of who will disclose the information and to whom it will be disclosed; an expiration date for the disclosure; a statement that the authorization can be revoked; a statement that disclosed information may be re-disclosed and no longer protected; a statement that if the individual does not provide an authorization, she/he may not be able to receive the intended treatment; the subject's signature and date.

AYUSH: Ayurveda, Yoga, Unani, Siddha and Homeopathy. Falls under the broad category of Indian Systems of Medicines and Homoeopathy (ISM&H) governed by Ministry of Health and Family Welfare, Government of India

[C]

CCD (Continuity of Care Document): A joint effort of HL7 International and ASTM. CCD fosters interoperability of clinical data by allowing physicians to send electronic medical information to other providers without loss of meaning and enabling improvement of patient care. CCD is an implementation guide for sharing Continuity of Care Record (CCR) patient summary data using the HL7 Version 3 Clinical Document Architecture (CDA), Release 2. It establishes a rich set of templates representing the typical sections of a summary record, and these same templates for vital signs, family history, plan of care, and so on can then be used for establishing interoperability across a wide range of clinical use cases.

CDT: Common Dental Terminology

Chain of Trust Agreement: A contract needed to extend the responsibility to protect health care data across a series of sub-contractual relationships.

Chief Complaint (CC), Reason for Consultation (RFC), Reason of Visit (ROV): for recording a patient's disease symptoms.

Client/Server Architecture: An information-transmission arrangement, in which a client program sends a request to a server. When the server receives the request, it disconnects from the client and processes the request. When the request is processed, the server reconnects to the client program and the information is transferred to the client. This usually implies that the server is located on site as opposed to the ASP (Application Server Provider) architecture.

Clinical Care Provider: Personnel or entities directly related to providing clinical care to patient.

Clinical Data Repository (CDR): A real-time database that consolidates data from a variety of clinical sources to present a unified view of a single patient. It is optimized to allow clinicians to retrieve data for a single patient rather than to identify a population of patients with common characteristics or to facilitate the management of a specific clinical department.

Clinical Decision Support System (CDSS): A clinical decision support system (CDSS) is software designed to aid clinicians in decision making by matching individual patient characteristics to computerized knowledge bases for the purpose of generating patient-specific assessments or recommendations.

GLOSSARY

Clinical Establishment: Clinical establishment means (1) a hospital, maternity home, nursing home, dispensary, clinic, sanatorium or an institution by whatever name called that offers services, facilities requiring diagnosis, treatment or care for illness, injury, deformity, abnormality or pregnancy in any recognized system of medicine established and administered or maintained by any person or body of persons, whether incorporated or not; or (2) a place established as an independent entity or part of an establishment referred to above, in connection with the diagnosis or treatment of diseases where pathological, bacteriological, genetic, radiological, chemical, biological investigations or other diagnostic or investigative services with the aid of laboratory or other medical equipment, are usually carried on, established and administered or maintained by any person or body of persons, whether incorporated or not. (Clinical Establishment Act – CEA 2010)

Clinical Guidelines (Protocols): Clinical guidelines are recommendations based on the latest available evidence for the appropriate treatment and care of a patient's condition.

Clinical Messaging: Communication of clinical information within the electronic medical record to other healthcare personnel.

Coded Data: Data are separated from personal identifiers through use of a code. As long as a link exists, data are considered indirectly identifiable and not anonymous or anonymized.

Code Set: Any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. This includes both the codes and their descriptions.

Coding: A mechanism for identifying and defining physicians' and hospitals' services. Coding provides universal definition and recognition of diagnoses, procedures and level of care. Coders usually work in medical records departments and coding is a function of billing. Medicare fraud investigators look closely at the medical record documentation, which supports codes and looks for consistency. Lack of consistency of documentation can earmark a record as "up-coded" which is considered fraud. A national certification exists for coding professionals and many compliance programs are raising standards of quality for their coding procedures.

Computer-Based Patient Record (CPR): A term for the process of replacing the traditional paper-based chart through automated electronic means; generally includes the collection of patient-specific information from various supplemental treatment systems, i.e., a day program and a personal care provider; its display in graphical format; and its storage for individual and aggregate purposes. CPR is also called "digital medical record" or "electronic medical record".

Computerized Patient Record (CPR): Also known as an EMR or EHR.A patient's past, present, and future clinical data stored in a server.

Computerized Physician Order Entry (CPOE): A system for physicians to electronically order labs, imaging and prescriptions

GLOSSARY

CPT (Current Procedural Terminology) Code: A recognizable five-digit number used to represent a service provided by a healthcare provider. It is a manual that assigns five digit codes to medical services and procedures to standardize claims processing and data analysis. The coding system for physicians' services developed by the CPT Editorial Panel of the American Medical Association.

[D]

Data Content: All the data elements and code sets inherent to a transaction, and not related to the format of the transaction.

Data: This is factual information (as measurements or statistics) used as a basis for reasoning, discussion, or calculation. It additionally points to the information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful.

Database Management System (DBMS): The separation of data from the computer application that allows entry or editing of data.

DICOM (Digital Imaging and Communications in Medicine): Digital Imaging and Communications in Medicine (DICOM) is a standard to define the connectivity and communication between medical imaging devices.

Disease Management: A type of product or service now being offered by many large pharmaceutical companies to get them into broader healthcare services. Bundles use of prescription drugs with physician and allied professionals, linked to large databases created by the pharmaceutical companies, to treat people with specific diseases. The claim is that this type of service provides higher quality of care at more reasonable price than alternative, presumably more fragmented, care. The development of such products by hugely capitalized companies should be the entire indicator necessary to convince a provider of how the healthcare market is changing. Competition is coming from every direction—other providers of all types, payers, employers who are developing their own in-house service systems, the drug companies.

Document Imaging: Is a process of converting paper documents into an electronic format usually through a scanning process.

Document Management: The Document Manager allows the medical institution to store vital patient documents such as X-Ray's, Paper Reports, and Lab Reports etc.

Documentation: The process of recording information.

DOHAD: Developmental Origins of Health and Diseases

Drug Formulary: Varying lists of prescription drugs approved by a given health plan for distribution to a covered person through specific pharmacies. Health plans often restrict or limit the type and number of medicines allowed for reimbursement by limiting the drug formulary list. The list of prescription drugs for which a particular employer or State Medicaid program will pay. Formularies are either "closed," including

only certain drugs or "open," including all drugs. Both types of formularies typically impose a cost scale requiring consumers to pay more for certain brands or types of drugs. See also Formulary.

Drug Formulary Database: This EMR feature is used for electronic prescribing, electronic medical record (EMR), and computerized physician order entry (CPOE) systems to present formulary status to the provider while during the prescribing decision.

DSM: Diagnostic and Statistical Manual for Mental Diseases

[E]

EDI: Acronym for Electronic Data Interchange. Electronic communication between two parties, generally for the filing of electronic claims to payers.

EDI Translator: Used in electronic claims and medical record transmissions, this is a software tool for accepting an EDI transmission and converting the data into another format, or for converting a non-EDI data file into an EDI format for transmission. See also Electronic Data Interchange.

EHR/EMR System Designer, Developer, Manufacturer, Vendor, Supplier, Retailer, Re-seller: Any entity that is involved in the design, development, testing, manufacturing, supplying, selling including re-selling of Electronic Health Records or Electronic Medical Records Systems as a whole or part thereof.

Electronic Data Interchange (EDI): The automated exchange of data and documents in a standardized format. In health care, some common uses of this technology include claims submission and payment, eligibility, and referral authorization. This refers to the exchange of routine business transactions from one computer to another in a standard format, using standard communications protocols.

Electronic Health Records (EHR): The one or more repositories, physically or virtually integrated, of information in computer processable form, relevant to the wellness, health and healthcare of an individual, capable of being stored and communicated securely and of being accessible by multiple authorized users, represented according to a standardized or commonly agreed logical information model. Its primary purpose is the support of life-long, effective, high quality and safe integrated healthcare. [ISO 18308:2011]

Electronic Medical Records (EMR): The EMR could be considered as special case of the EHR, restricted in scope to the medical domain or at least very much medically focused [ISO/TR 20514]. The Japanese Association of Healthcare Information Systems (JAHIS) has defined a five-level hierarchy of the EMR; Departmental EMR: contains a patient's medical information entered by a single hospital department (e.g. pathology, radiology, pharmacy); Inter-departmental EMR: contains a patient's medical information from two or more hospital departments; Hospital EMR: contains a patient's clinical information from a particular hospital; Inter-hospital EMR: contains a patient's medical information from two or more hospitals; EHR: longitudinal collection of health information from all sources. [Classification of EMR systems, JAHIS, V1.1, Mar 1996]

Electronic Protected Health Information (ePHI): Electronic Protected Health Information (ePHI) is any protected health information (PHI) that is created, stored, transmitted, or received electronically. Electronic

protected health information includes any medium used to store, transmit, or receive PHI electronically. The following and any future technologies used for accessing, transmitting, or receiving PHI electronically are covered. Media containing data at rest (data storage) like personal computers with internal hard drives used at work, home, or traveling, external portable hard drives, including iPods and similar devices, magnetic tape, removable storage devices, such as USB memory sticks, CDs, DVDs, and floppy disks, PDAs and smartphones and data in transit, via wireless, Ethernet, modem, DSL, or cable network connections, Email, File transfer. (For Protected Health Information – PHI, please see below)

Encounter: A clinical encounter is defined by ASTM as "(1) an instance of direct provider/practitioner to patient interaction, regardless of the setting, between a patient and a practitioner vested with primary responsibility for diagnosing, evaluating or treating the patient's condition, or both, or providing social worker services. (2) A contact between a patient and a practitioner who has primary responsibility for assessing and treating the patient at a given contact, exercising independent judgment." Encounter serves as a focal point linking clinical, administrative and financial information. Encounters occur in many different settings -- ambulatory care, inpatient care, emergency care, home health care, field and virtual (telemedicine).

Episode: An episode of care consists of all clinically related services for one patient for a discrete diagnostic condition from the onset of symptoms until the treatment is complete [http://www.ncmedsoc.org/non_members/pai/PAI-FinalWorkbookforVideo.pdf] Thus, for every new problem or set of problems that a person visits his clinical care provider, it is considered a new episode. Within that episode the patient will have one or many encounters with his clinical care providers till the treatment for that episode is complete. Even before the resolution of an episode, the person may have a new episode that is considered as a distinctly separate event altogether. Thus, there may be none, one or several ongoing active episodes. All resolved episodes are considered inactive. Hence they become part of the patient's past history. A notable point here is that all chronic diseases are considered active and may never get resolved during the life-time of the person, e.g., diabetes mellitus, hypertension, etc.

EPR: Broadly defined, a personal health record is the documentation of any form of patient information–including medical history, medicines, allergies, visit history, or vaccinations–that patients themselves may view, carry, amend, annotate, or maintain. Today, when we refer to PHRs, we typically mean an online personal health record–which may variously be referred to as an ePHR, an Internet PHR, an Internet medical record, or a consumer Internet Medical Record (CIMR). Generally, such records are maintained in a secure and confidential environment, allowing only the individual, or people authorized by the individual, to access the medical information. Not all electronic PHRs are Internet PHRs. PC-based PHRs may be set up to capture medical information offline.

Evidence Based Medicine: Evidence-based medicine (EBM) is the integration of best research evidence with clinical expertise to aid in the diagnosis and management of patients.

[F]

Family History: A list of the patient's family medical history including the chronic medical problems of parents, siblings, grandparents, etc.

FHIR: Fast Health Interoperable Resources, the newest version from HL7 org for messaging.

Formatting and Protocol Standards: Data exchange standards which are needed between CPR systems, as well as CPT and other provider systems, to ensure uniformity in methods for data collection, data storage and data presentation. Proactive providers are current in their knowledge of these standards and work to ensure their information systems conform to the standards.

Formulary: An approved list of prescription drugs; a list of selected pharmaceuticals and their appropriate dosages felt to be the most useful and cost effective for patient care. Organizations often develop a formulary under the aegis of a pharmacy and therapeutics committee. In HMOs, physicians are often required to prescribe from the formulary. See also Drug Formulary.

[G]

Growth Chart: A feature for a Primary Care or EMR that can be used for pediatric patients. Age, height, weight, and head measurements can be entered over the patient's lifetime, and the feature creates a line graph.

[H]

Health Care Operations: Institutional activities that is necessary to maintain and monitor the operations of the institution. Examples include but are not limited to: conducting quality assessment and improvement activities; developing clinical guidelines; case management; reviewing the competence or qualifications of health care professionals; education and training of students, trainees and practitioners; fraud and abuse programs; business planning and management; and customer service. Under the HIPAA Privacy Rule, these are allowable uses and disclosures of identifiable information “without specific authorization.” Research is not considered part of health care operations.

Health Care, Healthcare: Care, services, and supplies related to the health of an individual. Health care includes preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, among other services. Healthcare also includes the sale and dispensing of prescription drugs or devices.

Health Information: Information in any form (oral, written or otherwise) that relates to the past, present or future physical or mental health of an individual. That information could be created or received by a health care provider, a health plan, a public health authority, an employer, a general health insurer, a school, a university or a health care clearinghouse.

Health Level Seven (HL7): A data interchange protocol for health care computer applications that simplifies the ability of different vendor-supplied IS systems to interconnect. Although not a software program in itself, HL7 requires that each healthcare software vendor program HL7 interfaces for its products. The organization is one of the American National Standards Institute accredited Standard Developing Organization (SDO) - Health Level 7 domain is the standards for electronic interchange of clinical, financial and administrative info among healthcare oriented computer systems. Is a not-for-profit volunteer organization. It develops specifications, most widely used is the messaging standard that enables disparate health care applications to exchange key sets of clinical and administrative data. It promotes the use of standards within and among

healthcare organizations to increase the effectiveness and efficiency of healthcare delivery. It is an international community of healthcare subject matter experts and information scientists collaborating to create standards for the exchange, management and integration of electronic healthcare information.

Health: The state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity. It is recognized, however, that health has many dimensions (anatomical, physiological, and mental) and is largely culturally defined. The relative importance of various disabilities will differ depending upon the cultural milieu and the role of the affected individual in that culture. Most attempts at measurement have been assessed in terms or morbidity and mortality.

Healthcare provider: A health care provider is an individual or an institution that provides preventive, curative, promotional or rehabilitative health care services in a systematic way to individuals, families or communities. An individual health care provider may be a health care professional, an allied health professional, a community health worker, any or other person trained and knowledgeable in medicine, nursing or other allied health professions, or public/community health workers like , ASHA, ANM, midwives, paramedical staff, OT/lab/radio-diagnostic technicians, etc. An institution will include hospitals, clinics, primary care centers and other service delivery points of health care individual clinics, polyclinics, diagnostic centers, etc., i.e., any place where a medical record is generated during a patient-care provider encounter (in conformance to CEA 2010 – please refer to Clinical Establishment item above). It must be noted that any person solely performing non-clinical work is not a care provider.

Healthcare Service Provider (HSP): see Healthcare provider

History of Present Illness (HPI): The HPI is the history of the patient's chief complaint.

Human Subject: Refers to a living subject participating in research about whom directly or indirectly identifiable health information or data are obtained or created.

Hybrid Record: Term used for when a provider uses a combination of paper and electronic medical records during the transition phase to EMR.

[I]

IOD: Information Object Definition, pertains to DICOM

Independent Software Vendor (ISV): A company specializing in making or selling software products that runs on one or more computer hardware or operating system platforms.

Immunization: A complete list of all immunizations that the patient has had.

Informatics: The application of computer technology to the management of information.

Integration: Integration allows for secure communication between enterprise applications.

Interface: A means of communication between two computer systems, two software applications or two modules. Real time interface is a key element in healthcare information systems due to the need to access

patient care information and financial information instantaneously and comprehensively. Such real time communication is the key to managing health care in a cost effective manner because it provides the necessary decision-making information for clinicians, providers, other stakeholders, etc.

International Classification of Diseases: This is the universal coding method used to document the incidence of disease, injury, mortality and illness. A diagnosis and procedure classification system designed to facilitate collection of uniform and comparable health information. The ICD-9-CM was issued in 1979. This system is used to group patients into DRGs, prepare hospital and physician billings and prepare cost reports. Classification of disease by diagnosis codified into six-digit numbers. See also coding.

International Health Terminology Standards Development Organization (IHTSDO): Denmark-based organization that maintains and licenses SNOMED codes worldwide.

Interoperability: The capability to provide successful communication between end-users across a mixed environment of different domains, networks, facilities and equipment.

ISP: Internet Service Provider

ISV (Independent Software Vendor): An independent software vendor (ISV) is a company specializing in making or selling software, designed for mass or niche markets. This typically applies for application-specific or embedded software, from other software producers.

[J]

J-Codes: A subset of the HCPCS Level II code set with a high-order value of "J" that has been used to identify certain drugs and other items.

[L]

LAN (Local Area Network): A LAN supplies networking capability to a group of computers in close proximity to each other such as in an office building, a school, or a home.

Legacy System Integration: The integration of data between a legacy system and some other software program most commonly using HL-7 standards.

Legacy Systems: Computer applications, both hardware and software, which have been inherited through previous acquisition and installation. Most often, these systems run business applications that are not integrated with each other. Newer systems which stress open design and distributed processing capacity are gradually replacing such systems.

Length of Stay (LOS): The duration of an episode of care for a covered person. The number of days an individual stays in a hospital or inpatient facility. May also be reviewed as Average Length of Stay (ALOS).

LEPR (Longitudinal Patient Record): Longitudinal Patient Record is an EHR that includes all healthcare information from all sources.

[M]

Management Information System (MIS): The common term for the computer hardware and software that provides the support of managing the plan.

Master Patient / Member Index: An index or file with a unique identifier for each patient or member that serves as a key to a patient's or member's health record.

Maximum Defined Data Set: All of the required data elements for a particular standard based on a specific implementation specification. An entity creating a transaction is free to include whatever data any receiver might want or need. The recipient is free to ignore any portion of the data that is not needed to conduct their part of the associated business transaction, unless the inessential data is needed for coordination of benefits.

MCI: Medical Council of India

Medical Code Sets: Codes that characterize a medical condition or treatment. These code sets are usually maintained by professional societies and public health organizations. Compare to administrative code sets.

Medical Informatics: Medical informatics is the systematic study, or science, of the identification, collection, storage, communication, retrieval, and analysis of data about medical care services to improve decisions made by physicians and managers of health care organizations. Medical informatics will be as important to physicians and medical managers as the rules of financial accounting are to auditors.

Medical Management Information System (MMIS): A data system that allows payers and purchasers to track health care expenditure and utilization patterns. It may also be referred to as Health Information System (HIS), Health Information Management (HIM) or Information System (IS). See also Electronic Medical Record (EMR).

Metadata and Date Standard (MDDS) – A set of data elements and their specification for use in certain domain, such as health, e-governance.

MIMS: Monthly Index of Medical Specialties

Minimum Data Set: The minimum set of data elements that must be captured, stored, made available for retrieval, presentation, relay and sharing by an EHR system. It comprises of all of the essential data elements required for implementation. An entity creating a transaction must include the mandatory data elements at all times and is free to exclude optional data elements. The entity is free to additionally include whatever other data elements that any receiver might want or need. The recipient is free to ignore any portion of the data that is not mandatory and is further free to ignore any other portion of the data that is not needed to conduct their part of the associated transaction, unless required by sender, intermediaries or receiver. This minimum data set represents the most common data, and system designers are at liberty to add to it as they deem necessary to enrich or enhance their EHR systems.

Modifier: Additional character of a code added to an existing code that is used to help in extending or localization of the existing code.

[N]

NANDA: North American Nursing Diagnosis Association

National Council for Prescription Drug Programs: An ANSI-accredited group that maintains a number of standard formats for use by the retail pharmacy industry.

NEMA: The National Electrical Manufacturers Association (NEMA) is the association of electrical equipment and medical imaging manufacturers, founded in 1926 and headquartered in Rosslyn, Virginia.

Non-Participating Physician (or Provider): A provider, doctor or hospital that does not sign a contract to participate in a health plan, usually which requires reduced rates from the provider. In the Medicare Program, this refers to providers who are therefore not obligated to accept assignment on all Medicare claims. In commercial plans, non-participating providers are also called out of network providers or out of plan providers. If a beneficiary receives service from an out of network provider, the health plan (other than Medicare) will pay for the service at a reduced rate or will not pay at all.

[O]

Open Access: A term describing a member's ability to self-refer for specialty care. Open access arrangements allow a member to see a participating provider without a referral from another doctor. Health plan members' abilities, rights or invitation to self refer for specialty care. Also called Open Panel.

openEHR: openEHR is an open standard specification in health informatics that describes the management and storage, retrieval and exchange of health data in electronic health records (EHRs). In openEHR, all health data for a person is stored in a "one lifetime", vendor-independent, person-centered EHR. Maintained by the openEHR Foundation, these are based on a combination of years of European and Australian research and development into EHRs and new paradigms, including what has become known as the archetype methodology for specification of content and include information and service models for the EHR, demographics, clinical workflow and archetypes. They are designed to be the basis of a medico-legally sound, distributed, versioned EHR infrastructure.

OR: Operating Room – synonymous to OT as below

OT: Operation Theatre

OTC: Over the counter (drugs). Refers to those drugs that are available off the shelf without any prescription or advice from a registered medical practitioner

Outcome: A clinical outcome is the "change in the health of an individual, group of people or population which is attributable to an intervention or series of interventions". (Taken from: Frommer, Michael; Rubin, George; Lyle, David (1992)."The NSW Health Outcomes program". New South Wales Public Health Bulletin 3: 135. doi:10.1071/NB92067)

Outpatient Care: Care given a person who is not bedridden. It is also called ambulatory care. Many surgeries and treatments are now provided on an outpatient basis, while previously they had been considered reason for inpatient hospitalization. Some say this is the fastest growing segment of healthcare

[P]

Participating Physician: A primary care physician in practice in the payer's managed care service area who has entered into a contract.

Past History: A list of a patient's past health problems, surgeries and specialists.

Patient Demographics: All patient's pertinent information such as first and last name, SSN, DOB, insurance, etc.

Patient Portal: A secure web-based system that allows a patient to register for an appointment, schedule an appointment, request prescription refills, send and receive secure patient-physician messages, view lab results, pay their bills electronically, access physician directories.

Patient: A person who is under medical care or treatment

PC Based: A program designed to run on an individual PC. This typically means data is not shared in real time among other PCs (users).

PCP: Primary care physician who often acts as the primary gatekeeper in health plans. That is, often the PCP must approval referrals to specialists. Particularly in HMOs and some PPOs, all members must choose or are assigned a PCP.

PHR: A personal health record or PHR is typically a health record that is initiated and maintained by an individual. An ideal PHR would provide a complete and accurate summary of the health and medical history of an individual by gathering data from many sources and making this information accessible online.

Picture Archive Communication System (PACS): Used by radiology and diagnostic imaging organizations to electronically manage information and images

Practice Parameters, Practice Guidelines: Systematically developed statements to standardize care and to assist in practitioner and patient decisions about the appropriate health care for specific circumstances. Practice guidelines are usually developed through a process that combines scientific evidence of effectiveness with expert opinion. Practice guidelines are also referred to as clinical criteria, protocols, algorithms, review criteria, and guidelines. The American Medical Association defines practice parameters as strategies for patient management, developed to assist physicians in clinical decision-making. Practice parameters may also be referred to as practice options, practice guidelines, practice policies, or practice standards.

Prescription Drug: Drug that the law says can only be obtained by prescription.

Primary Care Physician: A "generalist" such as a family practitioner, pediatrician, internist, or obstetrician. In a managed care organization, a primary care physician is accountable for the total health services of enrollees including referrals, procedures and hospitalization. Also see Primary Care Provider.

GLOSSARY

Primary Care Provider: The provider that serves as the initial interface between the member and the medical care system. The PCP is usually a physician, selected by the member upon enrollment, who is trained in one of the primary care specialties who treats and is responsible for coordinating the treatment of members assigned to his/her plan.

Primary Care: Basic or general health care usually rendered by general practitioners, family practitioners, internists, obstetricians and pediatricians who are often referred to as primary care practitioners or PCPs. Professional and related services administered by an internist, family practitioner, obstetrician-gynecologist or pediatrician in an ambulatory setting, with referral to secondary care specialists, as necessary.

Principal Diagnosis: The medical condition that is ultimately determined to have caused a patient's admission to the hospital. The principal diagnosis is used to assign every patient to a diagnosis related group. This diagnosis may differ from the admitting and major diagnoses.

Privacy Standards: The Privacy standards restrict the use & disclosure of individually identifiable health information. Privacy standard applies to all protected health information may it is in physical or electronic form.

Privacy: Privacy means an individual's interest in limiting who has access to personal health care information. Specific patient authorization is required for use and disclosure of clinical notes. As per Fernando & Dawson, 2009, privacy is control of access to private information avoiding certain kinds of embarrassment and can be shared or not shared with others; Only authorized (by the patient) people can view the recorded data or part thereof

Progress Note: The documentation of a patient visit or encounter including all or part of the SOAP format.

Protected health information (PHI): Any individually identifiable information whether oral or recorded in any form or medium that is created, or received by a health care provider, health plan or health care Healthcare provider and relates to past, present, or future physical or mental health conditions of an individual; the provision of health care to the individual; or past, present, or future payment for health care to an individual.

[R]

Real Time: The instantaneous sharing of data among a user group. It is common to a client/server database configuration.

Reference Model (RM):

Referral: Some insurance companies require that on specific plans a referral must be obtained for certain procedures or visits to specialists. The referral is acquired by the primary care physician (PCP) by contacting the insurance company by phone or mail. This is a request for the service. The referral consists of an authorization code, a number of visits allowed (if applicable) and an expiration date.

Referring Provider: is the provider that referred the patient to a specialist or for a specific procedure.

Regenstrief: The Regenstrief Institute is an international non-profit medical research organization associated with Indiana University. It produces and maintains LOINC codes.

Relational Database: A database program that stores data in a manner similar to Excel, with the difference being the data elements are related (linked) to each other.

Remote Access: Data travels through a private, protected passage via the Internet, allowing healthcare providers to access from home or another practice location and allows EMR vendor to perform system maintenance off-site

Rendering/Performing Provider: The provider actually treating the patient.

Roles and Access Levels: The role and access level of the user needs to be determined and set by the system administrator. The role determines the access level. While roles may be such as system administrator, medical doctor, registered nurse, medical student, medical assistant, nurse assistant, ancillary nurse, health worker, Anganwadi worker (grass-root health worker), etc., the access levels may include viewing only, viewing/adding/editing only, viewing/adding/editing/deleting, all allowed etc. These need to be set out clearly in the SOP of the facility.

ROS (Review of Systems): A series of questions related to the system(s) that the patient is having complaints about (i.e. respiratory for cold symptoms).

RxNorm: RxNorm is the name of a US-specific terminology in medicine that contains all medications available on US market; it provides normalized names for clinical drugs and links its names to many of the drug vocabularies commonly used in pharmacy management and drug interaction software.

[S]

Secondary Care: Services provided by medical specialists who generally do not have first contact with patients (e.g., cardiologist, urologists, dermatologists). In the U.S., however, there has been a trend toward self-referral by patients for these services, rather than referral by primary care providers. This is quite different from the practice in England, for example, where all patients must first seek care from primary care providers and are then referred to secondary and/or tertiary providers, as needed.

Security Standards: The Security Standards require measures to protect the confidentiality, integrity and availability of e-PHI while it's being stored & exchanged. The security standard applies to all electronic PHI.

Security: This refers to the methods and techniques adopted to protect privacy and are a defense mechanism from any attack (Hong et al., 2004)

SNOMED: Systemized Nomenclature of Medicine Clinical Terms is the universal health care terminology. It is comprehensive and covers procedures, diseases, and clinical data. SNOMED CT helps to structure and computerize the medical record. It allows for a consistent way of indexing, storing, retrieving and aggregating clinical data across sites of care (i.e. hospitals, doctors offices) and specialties. By standardizing the

terminology, the variability in the way data is captured, encoded and used for clinical care of patients and research is reduced. Allows for more accurate reporting of data. It is currently available in English, Spanish and German.

Social History: A description of a patient's social habits and history including marital status, alcohol and drug use and exercise habits.

Solo Practice, Solo Practitioner: A physician who practices alone or with others but does not pool income or expenses. This form of practice is becoming increasingly less common as physicians band together for contracting, overhead costs and risk sharing.

SOP: Standard operating procedures or protocols

SQL: Structured Query Language – is a computer language aimed to store, manipulate and retrieve data stored in relational databases.

SDO: Standards Development Organization – an organization responsible for development and maintenance of a standard or several, usually run on a not-for-profit basis.

Subjective: Section in a progress note where a patient's account of their current problem is documented. Consists of chief complaint, HPI and ROS.

Sx: Abbreviation for symptoms

[T]

T1, T3 line: A high-speed internet connection provided via telephone lines often used by businesses needing internet connection speeds greater than DSL/Cable.

Therapeutic Alternatives: Strong Drug products that provide the same pharmacological or chemical effect in equivalent doses. Also see Drug Formulary.

TPA: Third Party Administrator

Treatment Episode: The period of treatment between admission and discharge from a modality, e.g., inpatient, residential, partial hospitalization, and outpatient, or the period of time between the first procedure and last procedure on an outpatient basis for a given diagnosis. Many healthcare statistics and profiles use this unit as a base for comparisons.

Treatment: The provision of health care by one or more health care providers. Treatment includes any consultation, referral or other exchanges of information to manage a patient's care.

[V]

Vital Statistics: Statistics relating to births (natality), deaths (mortality), marriages, health, and disease (morbidity). Vital statistics for the United States are published by the National Center for Health Statistics.

Vital statistics can be obtained from CDC, state health departments, county health departments and other agencies. An individual patient's vital statistics in a health care setting may also refer simply to blood pressure, temperature, height and weight, etc.

VPN: Virtual Private Network – A VPN "tunnel" is a secure connection, typically firewall to firewall that provides for remote access to your data server.

[W]

WADO: Web Access to DICOM Object Service.

WHO: The World Health Organization is a specialized agency of the United Nations that is concerned with international public health.

[X]

XML (Extensible Markup Language): Used for defining data elements on a Web page and communication between two business systems. Example: Standard messaging system for and EMR to integrate with another software such as a practice management or drug formulary database.

CONTACT INFORMATION

Contact Information

The Director (eGov)
e-Governance Division
Department of Health & Family Welfare
Ministry of Health & Family Welfare
Government of India
mohfw.nic.in

Implementation specific queries may be referred to:
National Release Center (NRC)
HPC-Medical & Bioinformatics Application Group,
Centre for Development of Advanced Computing (C-DAC)
Savitribai Phule Pune University Campus
Ganeshkhind Road
Pune – 411007
Email: nrc-help@cdac.in
http://www.snomedctnrc.in