Contents

➢ Executive Summary
➢ Standards at a Glance
➢ Health Record IT Standards
➢ Guidelines
➢ Data Ownership of Health Records
➢ Data Privacy and Security
➢ Glossary
➢ Way ahead
➢ Reference
EXECUTIVE SUMMARY
Introduction

- Ministry of Health & Family Welfare (MoH&FW) notified the Electronic Health Record (EHR) Standards for India in Sept 2013
- The notified standards were not only supported by professional bodies, regulatory bodies, stakeholders, but various technical and social commentators also
- Revised EHR Standards for India were notified in Dec 2016
For a health record of an individual to be clinically meaningful it needs to be from conception or birth, at the very least

Record of every clinical encounter (health-related event) can collectively 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

Purpose of collecting medical records, as much as possible, are manifold:

- Better and evidence based care
- Increasingly accurate and faster diagnosis
- Avoid repeating unnecessary tests
- Predictive analytics to support personalized care
- Improved health policy decisions
- Better understanding of the underlying issues
- All translating into improved personal and public health

Without standards, a *lifelong interoperable* medical record is hardly *interoperable*
Strategic Highlights

• EHR Standards for India (2016) provides a structured overview of the key EHR standards with respect to Indian healthcare system
• Detailed recommendation on the various aspects of EHR systems standardization perspective
• Short guideline regarding implementation specific to the item-in-context included
• It is understood that with proper adoption interoperability of both meaning and data can be achieved.

• **Aim:** 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
Goals

➢ Promote 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
STANDARDS AT A GLANCE
Architecture and Data Content

- Identification & Demographics
- Patient Identifiers
- Architecture Requirements
- Functional Requirements
- Reference Model and Composition
- Terminology
- Coding System
Information Exchange

- Imaging
- Scanned or Captured Records
- Data Exchange
- Other Relevant Standards
- Discharge/Treatment Summary
- E-Prescription
- Personal Healthcare and medical Device Interface
Access and Security

- Data Privacy and Security
- Information Security Management
- Privilege Management and Access Control
- Audit Trail and Logs
- Data Integrity
- Data Encryption
- Digital Certificate
Health Record
IT Standards

- Identification & Demographics
- Architecture & Functional Requirements
- Information Model
- Terminology & Coding
- Image, Multimedia, Waveform & Document
- Data Exchange
- Discharge Summary
- e-prescription
- Personal healthcare & Medical Devices Interfacing
- Principles of Data change
- Other Relevant Standards
Patient Unique Identifier is necessary in a health record system that identifies a patient

- UIDAI Aadhar Number (Preferred where available)
- Both of the following, if Aadhar is not available
  - Local Identifier (As per scheme used by HSP)
  - Any Central or state Government Issued Photo Identity Card Number

Links all artifacts and records of the patient

Recommended standards:

- MDDS- Demographic (Person Identification an Land Region Codification) Version 1.1 from E-Governance Standards, Govt. of India
A health record system must meet architectural requirements and functional specifications

- To meet the needs of service delivery
- Be clinically valid and reliable
- Meet legal and ethical requirements &
- Support good medical practices

Recommended standards:

- ISO 18308:2011 Health Informatics- Requirements for an Electronic Health Record Architecture

To be implemented as per scope/type of application
A health record system must accumulate observable data and information for all clinically relevant events and encounters.

Captured artefacts should have common semantic and syntactic logical information model and structural composition.

Standardized data capture makes it possible to communicate and exchange data across systems.

Recommended standards:

- ISO 13940 Health Informatics -System of Concepts to Support Continuity of Care
- ISO 13606 Health Informatics -Electronic Health Record Communication (Part 1 through 3)
- OpenEHR Foundation Models Release 1.0.2
  - Required Model Specifications: Base Model, Reference Model, Archetype Model
  - Optional Model Specifications: Service Model, Querying, Clinical Decision Support
Common terminology standard is necessary to:

- Have semantic interoperability between different health record systems
- Express unambiguous meaning of data captured, stored, transmitted, and analyzed

Coding Terminology standards are used for:

- Storing clinically relevant terms, observations, etc.

Classification and aggregation of infoRecoend standards:

- **Primary Terminology**: SNOMED CT
- **Test, Measurement and Observation Codes**: Logical Observation Identifiers Names and Codes (LOINC)
- **Classification Codes**: WHO Family of International Classifications (WHO-FIC)
  - **WHO ICD-10**: International Classification of Diseases (ICD)
  - **WHO ICF**: International Classification of Functioning, Disability and Health (ICF)
  - International Classification of Health Interventions (ICHI)
  - International Classification of Diseases for Oncology (ICD-O)
Cater to the need of data records and files of various types:

- Documentary records of various diagnostic
- Prescriptive data or information generated
- Image (series or single)
- Waveforms (ECG/EEG)
- Audio (such as Digital Stethoscope)
- Video (such as endoscope/USG etc.)

Recommended standards:

- NEMA Digital Imaging & Communication in medicine (DICOM) PS3.0 2015
- Image: JPEG lossy (or lossless) with size and resolution not less than 1024px x 768px at 300dpi
- Audio/Video: ISO/IEC 14496 – Coding of Audio Visual Objects

To be implemented as per scope/type/need of application
In-order to enable Data Exchange across healthcare systems, it is advisable to:

- Capture and provide as comprehensible medical information as possible
- Capture and retain information in standardized format

Recommended Standards (as applicable):

- EHR Archetypes: ISO 13606-5:2010 Health informatics - Electronic Health Record Communication - Part 5: Interface Specification [Also, refer to openEHR Service Model specification]
- Imaging/Waveform Exchange: NEMA DICOM PS3.0-2015 using DIMSE services & Part-10 media/files
Where not specifically provided, as a general rule, standards created or ratified by following Standard Development Organizations (SDOs) should be used:

- Bureau of Indian Standards and its MHD-17 Committee
- ISO TC 215 set of standards
- IEEE/NEMA/CE standards for physical systems and interfaces
Medical Council of India (MCI): Appendix - 3 of Code of Ethics Regulation 2002 (amended up to Feb-2016)

- Logical information model which includes data elements for discharge/treatment summary has to with the format as specified by MCI notification
- The printed reports should meet MCI prescribed formats whenever any discharge or treatment summary is prepared
Pharmacy Practice Regulations, 2015 Notification No. 14-148/ 2012-PCI by Pharmacy Council of India (PCI)

• Logical information model that includes data elements for e-Prescription has to satisfy requirements of the format for Medical Prescription as specified by the Pharmacy Council of India

• Electronic version should be digitally signed by a registered medical practitioner

• 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 & Medical Devices Interfacing

- Required for clinical data exchange, retrieval, storage, etc. for medical devices

- **Recommended standard:**
  - IEEE 11073 health informatics standards and related ISO standards
The data once entered into a health record system must become immutable.

Possible to update/append, provided:

- A complete audit trail of such change is maintained by the system.
- A new copy of data is created and original is retained through versioning.
The “As-Is Principal” requires that the data captured in the first instance should be retrievable at any given point of time later in same as it was provided during the time of record creation:

- Format
- Clarity
- Size and
- Detail

- No changes to original data after creation
- Changes in data can be in a copy, with versioning and due information to user or through SOP
Informed Format Change

- Change in data, format, or its nature in the system should be done with the explicit consent through:
  - Doctor / technician / person that is entering or managing the data
  - Set of preferences set by users

- The rule of conversion should be declared in the SOP of site/application
Guidelines

- Hardware
- Network & Connectivity
- Software Standards
- Health Record in Mobile Device
The IT hardware used should meet:

- Optimal requirements specified by the software used
- Relevant specifications from Medical and IT standards for the equipment

The following details should be planned and audited periodically:

- Backup or data preservation
- Data capacity
- System redundancy at various levels (disk, power, network, etc.)
- Network and Data security
- Capacity planning and quality requirements
Networking & Connectivity

➢ Should be able to harness any telecommunications-related connectivity such as LAN, WAN, Cloud etc.
➢ Ensure reliable and fast connectivity
➢ Ensure secure data exchange
➢ Ensure data exchange with data integrity
EHR system should ensure:

- Conformance to the specified standards & requirements
- Capturing, storing, retrieving, viewing, and analyzing healthcare records
- Interoperability
- Privacy, security and audit trail
- Search, merge, and demerge features
- Digital archiving of records of a person
There is an increasing demand for information delivery over mobile devices.

EHR data delivery applications on the mobile shall be governed by “Framework for Mobile Governance 2012” of MeitY, Government of India.

Essential health information over mobile device can be used for collecting:
- Demographics, medical condition, drug/allergy information, insurance info, medications, allergy and alerts, and vital signs
- Certain clinical and lifestyle related information from the patient

The information should be shared to extent relevant for emergency care and quick reference.
Data Ownership of Health Records

- Ethical, Legal, Social Issues
- Protected Health Information
- Data Ownership
- Data Access and Confidentiality
- Disclosure of Protected / Sensitive Information
- HSP Responsibilities
- Patient Privileges
- Denial of Information
- Data Preservation
- Patient Identity
- Legislation
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:
  
  Is created, or received by a stakeholder.
  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.

- e-PHI refers to any PHI that is created, stored, transmitted or received electronically

- Sensitive Information Includes:
  - Passwords
  - Financial information such as bank account or credit card or debit card or other payment instrument details
  - Physical, psychological and mental health condition
  - Sexual orientation
  - Medical records and history
  - Biometric information
  - Any detail relating to above received by the body corporate for provision of services
  - Any information relating to that is received, stored or processed by the body corporate under a lawful contract or otherwise
Data Ownership

- All health records generated by the healthcare provider, are held in trust by them on behalf of the patient
- All Protected health information contained in the EHR 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 themselves
Data Access & Confidentiality

➢ HSP to ensure confidentiality of the patient records

➢ Patients will have the sufficient privileges to:
  • Inspect and view their medical records without any time limit.
  • Restrict access to and disclosure of individually identifiable health information.
  • 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.

➢ Patient’s privileges to amend data shall be limited to correction of errors in the recorded patient/medical details.

➢ Audit trail to be strictly maintained for all changes.
Consent from patient or next of kin is necessary:

- **General:** For use in treatment, payments and other healthcare operations as defined by applicable laws by MCI
- **Specific:** Fair use for non-routine and non-health care purposes

Information disclosure without patient’s consent in the case of:

- Reporting notifiable/communicable diseases as mandated by law
- Complete record with all identifiers in an “as-is” state, on production of court order
- Totally anonymized data
Responsibility of a Healthcare Provider

➢ Protect and secure the stored health information, as per the guidelines
➢ Remove patient identifying information if it is not necessary to be provided
➢ Ensure informing the patient of policies related to their rights to health record privacy
➢ Document all its privacy policies and ensure that they are implemented and followed:
  • 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

- Patients can demand from a healthcare provider for:
  - A copy of the medical records held by that HSP (within 30 days of request)
  - To withhold, temporarily or permanently, specific information that he/she does not want disclosed to other organizations or individuals
  
  - Details of disclosures performed on the patient’s medical records for any reason whatsoever including:
    - 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

- Denial of the information to patient is possible on following grounds:
  - Information obtained from an anonymous source under a promise of confidentiality
  - Psychotherapy notes
  - Information compiled for civil, criminal or administrative action
All health records must compulsorily be preserved and not destroyed during the life-time of the person, ever.

Records may be turned to inactive status:

- Upon the demise of the patient (when there are no pending procedures, court cases)
- 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.

Analysis of health data of all persons is expected to greatly benefit in the understanding of health, disease processes and the amelioration thereof.
Patient Identifying Information

- Name
- Address (all geographic subdivisions smaller than street address, and PIN code)
- All elements of dates related to an individual (date of birth, date of death, etc.)
- Telephone, mobile, Fax numbers
- Email address
- Bank Account, 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
Existing Indian laws including IT Act 2000 and their amendments from time to time would prevail
Data Privacy and Security

- Security Technical Standards
- Administrative Safeguards
- Physical Safeguards
To implement reasonable and appropriate technical, administrative and physical 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
Security Technical Standards

➢ **Requirements Standard**
  • ISO/TS 14441:2013 Health Informatics – Security & Privacy Requirements of EHR Systems for Use in Conformity Assessment

➢ **Authentication**
  • Locally within the system/ Across the network

➢ **Automatic log-off**
  • An electronic session after a predetermined time of inactivity must be forcibly terminated

➢ **Overall information security management**
  • ISO 27799 Health informatics -Information Security Management in Health using ISO/IEC 27002
  • 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))
Privilege management and access control

- ISO 22600:2014 Health informatics -Privilege Management and Access Control (Part 1 through 3)
- Rule / policy based access is expected to give better control and flexibility in defining and enforcing access control
- Role Based, Policy Based, or Singular user are acceptable as long as conformant to applicable data security law(s) and rules

Audit log

- ISO 27789:2013 Health informatics -Audit Trails for Electronic Health Records
- All actions related to electronic health information must be recorded with the date, time, record identification, and user identification whenever created, modified (non-clinical data only), deleted (stale and non-clinical data only), or printed;
- An indication of which action(s) took place must also be recorded
Integrity
- It should be verifiable that Data is not altered during transmission
- Through Detection of events and Appropriate verification mechanisms
- *It is recommended that the Secure Hash Algorithm (SHA), SHA-256 or higher must be used*

Encryption
- Information must be encrypted and decrypted as necessary according to organization preferences and best available encryption key strength
- Data exchange must be through encrypted and integrity protected link
- *HTTPS, SSL v3.0, and TLS v1.2 standards should be used*

Digital Certificates
- *Use of Digital Certificate is for identification and digital signing is recommended in health record system*
- ISO 17090 Health informatics -Public Key Infrastructure (Part 1 through 5)
Administrative Safeguards Standards

• Healthcare providers should design, develop and implement standard operating procedure (SOP)

• **A healthcare provider must implement the following standards:**
  • 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
  • Evaluation, to evaluate an organization's security safeguards
Physical Safeguards Standards

- Required to protect electronic information systems
- Required physical standards are:
  - **Facility access control standard**: Limit actual physical access to electronic information systems and the facilities where they're located.
  - **Workstation use standard**: Control the physical attributes of a specific workstation or group of workstations, to maximize security.
  - **Workstation security standard**: Implement physical safeguards to deter the unauthorized access of a workstation.
  - **Device and media controls standard**: Control the movement of any electronic media containing ePHI from, to or within the facility.
GLOSSARY
Electronic Health Record (EHR)

• **Electronic Health record is a**
  • Computer processable information relevant to wellness, health and health care of an individual
  • Stored in one or more repositories
  • Integrated physically or virtually
  • Communicated securely
  • Accessible to multiple authorized users,
  • Represented using a Common logical information Model

• **Primary purpose is the support of life-long, effective, high quality and safe integrated healthcare**
Electronic Medical Records (EMR)

- **EMR** is a special case of **EHR** that holds records specific to the scope to the medical domain
  - **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
Electronic Protected Health Information (ePHI)

- 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.
- All technologies used for accessing, transmitting, or receiving PHI electronically are covered under e-PHI
  - Media containing data at rest (data storage) like personal computers with internal hard drives, external portable hard drives, magnetic tape, removable storage devices
  - Data in transit, via wireless, Ethernet, modem, DSL, or cable network connections, Email, File transfer
MoH&FW moved ahead with facilitating the adoption of EHR Standards, as next steps:

- SNOMED CT made available free-for-use in India
- Set-up of National Release Center (NRC) for widespread adoption and support of SNOMED CT in country
- National Resource Centre for EHR Standards (NRCeS) to support adoption and implementation of EHR Standards for India

For any queries, assistance, implementation support related to EHR Standards for India (2016) contact NRCeS at nrc-help@cdac.in
References

▪ ELECTRONIC HEALTH RECORD (EHR) STANDARDS FOR INDIA (2016), Standards Set Recommendations v2.0, e-Health Division, Department of Health & Family Welfare, Ministry of Health & Family Welfare, Government of India
http://www.mohfw.nic.in/sites/default/files/17739294021483341357.pdf
Thank You

nrc-help@cdac.in