Owl Health&Care Technologies | A business unit of ValueMomentum

Comprehensive Enterprise Data Standards for ONC Interoperability Compliance

Ensuring ONC interoperability compliance requires a structured approach to enterprise data standards across various domains, including data exchange formats, security, governance, clinical terminologies, APIs, and compliance monitoring. Below is a deep dive into each key area.

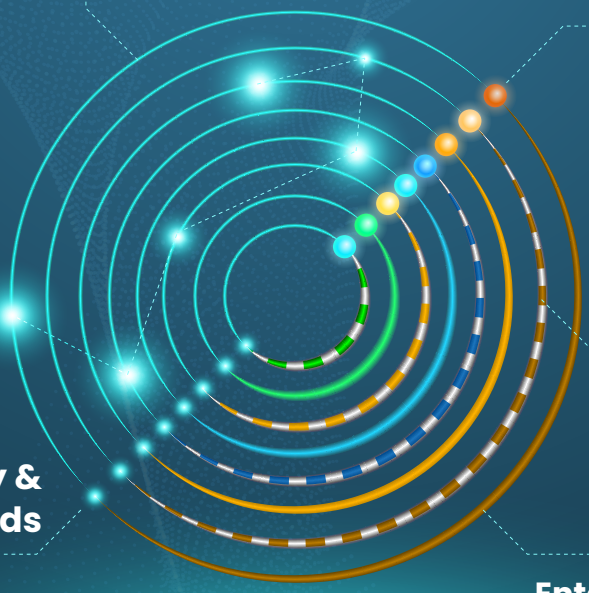

TABLE OF CONTENTS

OwlHealth&Care sets the standard in healthcare interoperability, delivering unmatched data quality and comprehensive lifecycle management that ensure seamless compliance and enhanced operational efficiency.

1. DATA EXCHANGE & INTEROPERABILITY STANDARDS

The **ONC 21st Century Cures Act** mandates seamless data exchange across healthcare providers, payers, and patients. This is achieved through:

a. **HL7 FHIR (Fast Healthcare Interoperability Resources)**
   FHIR is the **primary standard** for data interoperability in modern healthcare IT systems. Key FHIR requirements include:
   1. **FHIR R4 (Release 4) Adoption** – Required by ONC and CMS for APIs.
   2. **FHIR RESTful APIs** – Ensures structured, web-based access to clinical data.
   3. **FHIR Resources:**
      i. **Patient** (demographics, identity)
      ii. **Observation** (lab results, vitals)
      iii. **MedicationRequest** (prescriptions)
      iv. **AllergyIntolerance** (allergy history)
      v. **Condition** (chronic diseases, acute conditions)
   4. **FHIR Bulk Data API** – Required for population-level health data sharing.
   5. **FHIR Provenance Resource** – Tracks data lineage, sources, and modifications.

b. **Consolidated Clinical Document Architecture (C-CDA)**
   Although FHIR is the standard for **modern** interoperability, **C-CDA** remains **essential for legacy EHR systems**. Used for:
      i. **Continuity of Care Document (CCD)**
      ii. **Progress Notes**
      iii. **Discharge Summaries**
      iv. **Consultation Notes**
      v. **Referral Summaries**

c. **US Core Data for Interoperability (USCDI)**
   ONC mandates **USCDI** as the **minimum dataset** for interoperability, which includes:
      i. **Patient Demographics** (name, DOB, sex, race, ethnicity)
      ii. **Clinical Data** (vitals, medications, lab results, procedures)
      iii. **Care Team Members** (attending physicians, specialists)
      iv. **Allergies and Medications**
      v. **Health Insurance and Coverage**
      vi. **Advance Directives and Clinical Notes**

d. **eHealth Exchange & TEFCA (Trusted Exchange Framework and Common Agreement)**
      i. **TEFCA ensures nationwide health information exchange.**
      ii. Supports **Qualified Health Information Networks (QHINs).**
      iii. Requires **data sharing agreements** with **Health Information Exchanges (HIEs).**

2. STANDARDIZED HEALTHCARE TERMINOLOGIES & CODE SETS

To ensure **semantic interoperability**, all exchanged data must use standard vocabularies. The most common enterprise data standards include:

a. Clinical Data Standardization

Standard	Purpose
SNOMED CT	Used for clinical conditions, procedures, and symptoms.
ICD-10-CM	Standard for disease classification and diagnosis coding.
ICD-10-PCS	Standard for procedure coding.
LOINC (Logical Observation Identifiers Names and Codes)	Standardized lab test and diagnostic results.
RxNorm	Standardized naming for medications and drugs.
NDC (National Drug Codes)	Standard for identifying pharmaceuticals.
CPT (Current Procedural Terminology)	Standard for medical billing and procedure codes.

b. Data Mapping Between Terminologies

To ensure **cross-compatibility,** data must be mapped between different standards. Examples:

i. **SNOMED CT → ICD-10** (for claims processing)

ii. **LOINC → FHIR Observations** (for lab test results)

iii. **RxNorm → FHIR MedicationRequest** (for prescriptions)

3. ENTERPRISE DATA MODELING & STRUCTURING STANDARDS

a. Common Data Models (CDM)

i. **OMOP (Observational Medical Outcomes Partnership) CDM -** Standardized data model used for research and analytics.

ii. **PCORnet CDM -** Used for clinical trials and patient-centered outcomes.

iii. **i2b2 (Informatics for Integrating Biology & the Bedside) -** Used for clinical research.

b. Data Normalization & Standardization

i. **Enterprise-wide data dictionaries** should be maintained.

ii. **Data provenance and metadata tagging** must be enforced.

iii. **Normalization rules** should be applied across disparate EHR and payer systems.

4. API, SECURITY & AUTHENTICATION STANDARDS

a. ONC API Compliance Standards

i) **FHIR APIs for Patient Access** – Ensuring ONC-mandated API access for patients.

ii) **FHIR Bulk Data Export APIs** – Required for population-level data analytics.

iii) **FHIR Subscription API** – Real-time event notifications for providers.

b. Authentication & Authorization

i) **OAuth 2.0 and OpenID Connect** – Required for user authentication.

ii) **SMART on FHIR** – Enables secure authentication for third-party apps.

iii) **FHIR Consent Resource** – Ensures patient-driven data access controls.

c. Data Security & Privacy

Standard	Purpose
HIPAA	Ensures patient data security and privacy.
NIST Cybersecurity Framework	Establishes security controls and risk management.
SOC 2 Compliance	Ensures secure handling of healthcare data.

5. ENTERPRISE DATA GOVERNANCE & MASTER DATA MANAGEMENT

a. Data governance involves several critical components:

i) Data Quality Management (DQM)

To ensure data integrity and consistency, organizations must implement:

- **Automated Data Validation Rules:** Verifying data format, accuracy, and completeness.
- **Data Cleansing Processes:** Identifying and correcting duplicate, missing, or inconsistent data.
- **Data Profiling & Audits:** Regularly assessing data quality and usability.

Example Data Quality Metrics:

- **Completeness:** % of records with missing fields (e.g., missing patient demographics).
- **Accuracy:** % of correctly coded diagnoses/procedures.
- **Consistency:** Data remains uniform across systems (e.g., patient data is the same across EHRs).
- **Timeliness:** Data is updated in real-time or near real-time.

ii) Master Data Management (MDM)

Enterprise Level Master Patient / Member Index

- Prevents duplicate or mismatched patient records across different systems.
- Uses probabilistic, deterministic, or hybrid matching algorithms to link patient records from different sources.
- Supports patient matching via unique identifiers (e.g., Patient ID, SSN, biometrics, FHIR Provenance).

Provider Directory Management

- Maintains accurate provider information (credentials, affiliations, specialty).
- Aligns with NPPES (National Plan and Provider Enumeration System) for standardization.
- Ensures provider identity verification via National Provider Identifier (NPI).

5. ENTERPRISE DATA GOVERNANCE & MASTER DATA MANAGEMENT CONT.

Payer & Claims Data Management

- Ensures standardized payer and claims data formats (X12, FHIR-based APIs).
- Maintains accurate benefit eligibility records.
- Enables interoperability with Health Information Exchanges (HIEs).

iii) Metadata & Data Provence Standards

Metadata is essential for data traceability, governance, and compliance.

- FHIR Provenance Resource: Tracks who created, accessed, or modified data.
- Standardized metadata tagging ensures interoperability across systems.

Data Provenance & Lineage: Data lineage helps track the source, transformation, and usage of data.

- Provenance tracking ensures auditability and accountability.
- ONC mandates transparent data origins for exchanged health data.

Example: A patient's lab result (LOINC code) should include:

- Source System (EHR, lab, HIE)
- Date & Time Captured
- Modifications & Ownership
- Access History

iv) Security & Privacy Compliance

Healthcare organizations must ensure compliance with HIPAA, ONC, and CMS regulations for data privacy and security.

- Data Access & Role-Based Permissions
  - Role-Based Access Control (RBAC) ensures only authorized personnel can access specific data.
  - FHIR Consent Resource allows patients to control access to their data.
- Secure APIs & Authentication
  - OAuth 2.0 & OpenID Connect for patient authentication.
  - SMART on FHIR framework for secure third-party app access.
  - FHIR-based consent management ensures patient control over shared data.
- HIPAA & NIST Compliance
  - HIPAA Security Rule: Protects PHI (Protected Health Information) from unauthorized access.
  - NIST Cybersecurity Framework: Provides risk management and security guidelines.

5. ENTERPRISE DATA GOVERNANCE & MASTER DATA MANAGEMENT CONT.

v) Data Access & Interoperability Controls

Interoperability via API-Driven Access: To comply with ONC's Final Rule, organizations must:

- Implement FHIR-based APIs for real-time data exchange.
- Allow patients to access their EHRs without special effort.
- Support third-party apps connecting via SMART on FHIR APIs.

Information Blocking Prevention

- Ensure full compliance with ONC's information blocking rules.
- Prevent excessive restrictions on third-party data access.

vi) Regulatory Compliance & Auditing

To ensure ONC interoperability compliance, organizations must adhere to:

i) ONC Health IT Certification
   - Certifies EHR systems and APIs for interoperability.
   - Requires FHIR R4, USCDI, and HIPAA compliance.

ii) Quality Reporting & Analytics
   - FHIR MeasureReport Resource ensures clinical quality measure reporting.
   - CMS Quality Payment Program (QPP) Reporting for regulatory compliance.

iii) Audit Logging & Data Monitoring
   - Maintain an immutable audit trail for all patient data transactions.
   - Monitor access logs to detect unauthorized access.

vii) Data Lifecycle Management

i) Data Retention Policies
   - Align with state & federal regulations (e.g., 6-10 years for PHI).
   - Define archival policies for inactive patient records.

ii) Data Deletion & De-Identification
   - Ensure secure PHI deletion processes.
   - Apply de-identification techniques (Safe Harbor, Expert Determination) before sharing patient data.

5. ENTERPRISE DATA GOVERNANCE & MASTER DATA MANAGEMENT CONT.

Summary of Governance Topics:

Pillar	Objective
1. **Data Standardization & Interoperability**	Ensure data consistency across healthcare systems using ONC-approved standards (FHIR, USCDI, SNOMED, etc.).
2. **Data Quality & Master Data Management (MDM)**	Ensure high-quality, deduplicated, and unified patient, provider, and payer data.
3. **Security, Privacy & Compliance**	Protect patient data per HIPAA, NIST, and ONC guidelines with RBAC and secure APIs.
4. **Data Access, API Governance & Information Blocking Prevention**	Define policies for secure, role-based data access, FHIR APIs, and ONC information blocking compliance.
5. **Regulatory Compliance & Auditability**	Ensure adherence to ONC Health IT Certification, HIPAA, and CMS Quality Reporting.
6. **Data Lifecycle Management**	Define data retention, archival, and PHI de-identification strategies.

6. COMPLIANCE, AUDITING & REPORTING STANDARDS

a. Health Information Exchange (HIE) Participation
   i) Ensures compliance with regional and national HIE networks.
   ii) Requires EHR system certification under ONC Health IT Certification Program.

b. Quality Reporting & Analytics Standards
   i) FHIR MeasureReport Resource for clinical quality measures.
   ii) CMS Quality Payment Program (QPP) Reporting.

c. Information Blocking Prevention
   i) Ensures full compliance with ONC's information blocking rules.
   ii) Prevents excessive restrictions on third-party data access.

ABOUT OWLHEALTH&CARE

At Owlhealth&Care, we enhance member loyalty, engagement, and satisfaction through advanced technology that modernizes systems and processes for a superior user experience. We personalize interactions for every stakeholder, improving our star ratings and leading to enhanced reimbursements. Using sophisticated data analytics, we identify trends, predict risks, and make informed decisions on care management and cost efficiency. Committed to compliance, our integration technologies streamline health information management and facilitate seamless communication across all stakeholders.

www.owlhealth.com
info@owlhealth.com
908-755-0010

Owl Health&Care Technologies
A business unit of ValueMomentum