1. Firme elettroniche

Consentono di garantire la **paternità** di un documento digitale o di un’azione svolta

Un **documento** è qualsiasi mezzo, soprattutto grafico, che provi l’esistenza di un fatto, l’esattezza o la verità di un’asserzione. Un **documento informatico** è la **rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. L’Italia** è stato il primo paese europeo ad aver attribuito piena **validità giuridica** ai documenti informatici.

**eIDAS**: electronic IDentification Autentication and Signature

Regolamento eIDAS sull’identità digitale: fornisce una **base normativa comune** per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni e incrementa la **sicurezza** e **l’efficacia** dei servizi elettronici e delle transazioni di e-business e commercio elettronico nell’Unione Europea. Prevede varie tipologie di firma elettronica (dalla più debole alla più forte):

* **Firma elettronica** (semplice) (FE)
  + Assume il valore di strumento esclusivo di **sottoscrizione**
  + **Non prevede meccanismi di autenticazione** del firmatario o di integrità del dato firmato
  + Esempi: PIN, o username e password; scansione di firma cartacea; messaggio di posta elettronica ordinaria; firma biometrica
  + Valore: è una sottoscrizione di principio che non fa riferimento ad alcun prodotto o servizio
    - **Non** è possibile comprovarne **l’autenticità**, solo l’autorità giudiziaria ha facoltà di dichiarare autentica o meno questo tipo di firma, in base a valutazioni di sicurezza, integrità e immodificabilità
  + I **programmi applicativi** nelle **aziende sanitarie** richiedono autenticazione all’accesso
    - Login con username e password
    - Gli operatori sanitari appongono una firma elettronica semplice su ogni operazione effettuata al computer
* **Firma elettronica Avanzata** (FEA)
  + È connessa unicamente al firmatario ed è idonea ad **identificarlo**
  + È **creata mediante dati per la creazione di una firma elettronica** che il firmatario può, con un elevato livello di sicurezza, controllare
  + È **collegata ai dati sottoscritti** in modo da consentire l’identificazione di ogni successiva **modifica** di tali dati
  + Esempio: **firma grafometrica**
    - Una tipologia di FEA realizzata con un gesto manuale del tutto analogo alla firma autografa su carta acquisito da un dispositivo in grado di acquisire dinamicamente il movimento di uno stilo
    - Vengono memorizzate non solo l’immagine, ma anche alcune caratteristiche biometriche come velocità, pressione, accelerazione
  + Formati:
    - **PAdES**: PDF
    - **XAdES**: XML
    - **CAdES**: CMS
    - ASiC: associated signature container
* **Firma elettronica Qualificata** (FAQ)
  + È basata su un **certificato qualificato per firme elettroniche** emesso da **un’autorità indipendente e riconosciuta**, garantisce **l’identità** del firmatario e **l’integrità** del documento firmato (assenza di modifiche)
  + **Dispositivo sicuro di firma**: token o smart card
  + Ad una firma elettronica non possono essere negati gli **effetti giuridici** e l’ammissibilità come prova in procedimenti giudiziali, avendo effetti giuridici equivalenti a quelli di una firma autografa.
  + È riconosciuta come **firma elettronica qualificata in tutti gli Stati membri**
  + Esempio: **firma digitale**
    - Un particolare tipo di firma qualificata basata su un sistema di **chiavi crittografiche**, una **pubblica** e una **privata**, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e un soggetto terzo tramite la chiave pubblica, rispettivamente di **rendere manifesta** e di **verificare la provenienza e l’integrità di un documento informatico** o di un insieme di documenti informatici
    - Proprietà:
      * **Autenticità**: permette di dimostrare l’identità e la paternità del firmatario
      * **Non ripudio**: il firmatario non può disconoscere un file da lui digitalmente firmato
      * **Integrità**: è possibile accettare se un file, dopo la firma digitale, sia stato modificato (?)
    - Tecnologia utilizzata:
      * **Crittografia a chiavi asimmetriche** (chiave pubblico/privata): garantisce la **riservatezza** del contenuto dei messaggi, rendendoli incomprensibili a chi non sia in possesso di una chiave per interpretarli. Ad ogni attore coinvolto è associata una coppia di chiavi
        + **Pubblica**: deve essere distribuita pubblicamente
        + **Privata**: è personale e deve essere mantenuta segreta

Perché il sistema risulti sicuro è necessario che solo l’utente stesso e nessun altro abbia accesso alla chiave privata. Per ogni utente le due chiavi vengono generate da un apposito **algoritmo** con la garanzia che la chiave privata sia la sola in grado di decifrare correttamente i messaggi cifrati con la chiave pubblica associata e viceversa

* + - * **Certificato digitale**
        + **Documento elettronico che attesta l’associazione univoca di un soggetto con la chiave pubblica** che dichiara di utilizzarla nell’ambito di procedure di cifratura asimmetrica e/o autenticazione. Contiene **informazioni sulla chiave pubblica, identità del proprietario e sull’emittente del certificato**
        + La **chiave privata** è di solito inserita nel **Dispositivo sicuro di firma:** il token o la smart card
    - La firma digitale consiste nella creazione di un file definito **busta crittografica,** che racchiude al suo interno
      * Il **documento originale**
      * **L’evidenza informatica della firma**
      * La **chiave per la verifica** della stessa che, a sua volta, è contenuta nel certificato emesso a nome del sottoscrittore
        + L’autenticità del certificato è garantita da un’autorità di certificazione in Italia
    - **Firma digitale remota**: è una tipologia di firma digitale accessibile via **rete** per cui **la chiave privata è conservata assieme al certificato di firma all’interno di un server remoto sicuro** da parte di un **certificatore accreditato**
      * Il **firmatario è identificato dal servizio** e autorizza l’apposizione della firma tramite un meccanismo di sicurezza (PIN, token OTP, riconoscimento grafometrico della firma autografa, telefono cellulare come OTP seguito da PIN firma)

**Marca temporale**: è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. Può essere utilizzato anche su file non firmati digitalmente, garantendone una collocazione temporale certa e legalmente valida

1. Posta elettronica certificata (**PEC**)

Consente di trasmettere documenti digitali replicando e migliorando i meccanismi della raccomandata cartacea. È un tipo particolare di posta elettronica che permette di **dare a un messaggio di posta elettronica lo stesso valore legale di una tradizionale raccomandata**, garantendo la prova di invio e di consegna. Garantisce la **paternità** e il **non ripudio** della trasmissione. È **obbligatoria** per tutti i professionisti iscritti ad **albi** e le **aziende pubbliche**.

Flusso della PEC

1. Al momento di invio del messaggio, il **gestore di posta certificata del mittente** (GM) fornisce al mittente stesso una **ricevuta di accettazione**. In essa sono contenuti dati di certificazione che costituiscono prova dell’avvenuta spedizione.
2. Successivamente, il GM inoltra la PEC al **gestore del destinatario** (GD). Quest’ultimo rilascia al primo una **ricevuta** che attesta la **presa in carico del messaggio**. Quindi il GD deposita la PEC nella casella del destinatario ed invia al mittente una **ricevuta di consegna**, con indicazione temporale. Le tre ricevute sono firmate con firme digitali.
3. Qualora il GM non abbia ricevuto da GD nelle 12 ore successive all’inoltro, la ricevuta di presa in carico o di avvenuta consegna, comunica al mittente che il GD potrebbe non essere in grado di effettuare la consegna del messaggio con rilascio di diverse tipologie di avviso

Vantaggi:

* Certifica **l’identità** del mittente, la **consegna** e **l’integrità** del messaggio
* La trasmissione avviene in forma **criptata**, particolarmente importante per il trattamento di dati sensibili
* È supportato **ogni** **formato digitale**
* La PEC è **semplice** da usare, ha **velocità** superiore e **costi** inferiori, rispetta elevati requisiti di **qualità** e **continuità** del servizio
* Il gestore di PEC ha l’obbligo di archiviare tutti gli eventi associati a invii e ricezioni dei messaggi per almeno 30 mesi, e di garantire il rispetto delle misure di sicurezza e riservatezza
* I messaggi PEC sono **malware free**

Punti critici:

* Non è riconosciuta a **livello europeo**
* Non vi sono opzioni **gratuite** per il suo utilizzo
* Il fatto che la data di notifica del file depositato coincida con la data del deposito comporta la necessità di monitorare regolarmente la propria casella di posta certificata
* La comunicazione ha **valore legale** solo se avviene tra caselle PEC

Sistemi di classificazione e codifica in ambito medico

**Sistema informatico sanitario**

* **Infrastruttura**: hardware, software e reti dati
* **Dati, informazioni, conoscenze**
* **Processi**: tutte le attività di produzione ed utilizzo di dati
* **Persone** che sovraintendono a tali processi

**Codificare un dato**

Codificare un dato significa esprimerlo mediante **regole e simboli di un sistema convenzionale** (il codice), stabilito concordemente dall’emettitore e dal ricevitore del dato, allo scopo di gestire, trasmettere o elaborare le informazioni o, talora, di mantenerle segrete.

Nella codifica dei dati è fortemente consigliato l’uso di un “**formato aperto**”; in informatica tale locuzione indica una specifica tecnica di **pubblico dominio**, utilizzata per la descrizione e l'archiviazione di dati digitali, libera da restrizioni legali per il suo utilizzo.

Caratteristiche dei sistemi di codifica

* i sistemi di codifica permettono di assegnare un significato univoco ai termini (la **semantica**);
* il significato dei termini si deve conservare nel tempo, mediante l’uso di un dizionario: è **sconsigliata** la “**risemantizzazione**";
* i codici devono avere un **significato condiviso**;
* i termini codificati devono poter essere **facilmente** **classificati** (per questo i codici hanno una struttura studiata per una determinata classificazione);

Importanti classificazioni in ambito sanitario

1. **ICD** – International Classification of Diseases: È un sistema di classificazione internazionale delle **malattie**, dei **traumatismi** e delle **procedure diagnostico terapeutiche**

* È uno standard sviluppato **dall’OMS** con **organizzazione gerarchica**
* Storia: lo studio statistico delle patologie ebbe inizio nel **1600** con i lavori di **Graunt**, statistico londinese che studiò la **mortalità infantile**. Successivamente il medico francese **Bertillon** realizzò una classificazione delle cause di morte che venne utilizzata in molti paesi prendendo il nome di **ICD**. Nel **1975** l’OMS approva la **9° revisione** della classificazione ICD detta appunto ICD9, usata oggi in Italia e in tutto il mondo. Sono attualmente già disponibili le versioni ICD10 e ICD11, che però presentano delle problematiche. ICD9 era nata per classificare i casi di mortalità. **ICD9 – CM** è la Clinical Modification dell’ICD9 che introduce anche la classificazione delle procedure e i dati di morbosità.
* La traduzione italiana è predisposta **dall’ISTAT**
* È utilizzata nelle **schede di dimissione ospedaliera** (obbligatorio) e nella **codifica delle diagnosi del profilo sanitario sintetico**
* Assegna ai termini medici in cui sono espresse le diagnosi, le procedure, le cause etc. **codici alfanumerici**
* Permette di **conservare nel tempo e nello spazio** il significato dei termini medici grazie ad un **linguaggio condiviso** che favorisce la comunicazione in modo corretto, **senza ambiguità**
* **Specificità**: riguarda un ambito specifico, quello sanitario
* **Completezza** ed **esaustività**: da sola basta per indicare tutto ciò che serve
* **Revisioni annuali**: vengono inseriti nuovi codici o meglio specificati quelli esistenti, quelli vecchi non sono cancellati per non perdere la storia, **è vietata la risemantizzazione**
* **Evitare errori:** controlli automatici del software impediscono di inserire codici inappropriati o contraddittori con alcune informazioni del paziente
* **Organizzazione**: due classificazioni
  + Una per le **patologie**: da 3 a 5 caratteri numerici o alfanumerici. Più caratteri = più dettagliato
  + Una per le **procedure**: da 2 a 4 caratteri numerici

Ognuna suddivisa in due sezioni

* + **Indice alfabetico**
  + **Elenco sistematico**
* I codici sono **ordinati**, per finalità statistiche, in gruppi tra loro correlati, la loro suddivisione segue l’asse **eziologico** ed **anatomico**
* Due classificazioni supplementari:
  + **Codici V** – fattori che influenzano lo stato di salute
  + **Codici E** – cause esterne di traumatismo ed avvelenamento

1. **SNOMED** – Systematized Nomenclature of Medicine: SNOMED è una **raccolta di termini medici** che contiene codici, termini, sinonimi e definizioni utilizzati nella **documentazione clinica**. È considerata la **terminologia clinica multilingue più completa al mondo** (non è solo patologie e procedure come ICD9). SNOMED è come un ampio **vocabolario** contenente termini tecnici usati in medicina, ad ognuno dei quali è associato un **codice**, il cui obiettivo è di classificare ed elencare tutti gli elementi che compongono il linguaggio medico in una raccolta sistematica di nomi con annesso il proprio significato. Ciò ha ripercussioni **sull'efficienza delle cure**, sulla **sicurezza** dei pazienti, sulla **sostenibilità** dei servizi sanitari, sulla **interoperabilità** dei sistemi informativi sanitari.

* Storia: nacque nel **1965** con il nome **SNOP**; **SNOMED CT** (Clinical Terms) arriva nel **1999** dalla fusione e ristrutturazione di SNOMED RT e CTV3. Il prodotto finale è stato rilasciato ne **2002**. Inizialmente era protetto da **copyright** e l’uso era a **pagamento**. Dal **2007** la proprietà intellettuale è passata **all’International Health Terminology Standards** **Development Organization** che ne promuove **l’uso** e la **diffusione**
* SNOMED vs ICD9
  + Differenze strutturali:
    - **ICD9** contiene un insieme di **codici poco legati tra loro,**
    - **SNOMED** contiene una fitta **rete di relazioni tra i codici**.
  + Finalità:
    - **ICD9** è nata per fare **statistiche**, report, studi epidemiologici, calcolo di costi.
    - **SNOMED** si presta di più a fare **analisi** ed essere usata come base per programmi di **supporto alle decisioni**
  + Per fare ricerche in SNOMED CT si può fare una **query** su un DB; su ICD9-CM si può fare un **filtro sui termini** che poi devono essere **analizzati manualmente**
  + SNOMED non è in concorrenza con ICD9, bensì le due classificazioni **si completano**, sono usate nello stesso ambito ma con scopi differenti.
* Vantaggi
  + Un sistema di codici accettati e verificati a livello internazionale permette lo **scambio di informazioni indipendentemente dalla lingua**
  + Facilitare la **ricerca** dei dati, la ricerca medica, la **qualità** delle cure e lo **sviluppo** di Enterprise Health Record (EHR).
  + Permette di **registrare facilmente i dati** e successivamente di accedere a livelli di aggregazione differenti
* Proprietà e caratteristiche
  + **Specificità**: rappresentano concetti singoli, unitari relativi all’ambito sanitario
  + **Completezza**: consente la descrizione di qualunque situazione, ogni anno è revisionata e ampliata
* SNOMED CT **cerca di usare lo stesso linguaggio dei clinici**
* SNOMED è un sistema di codifica **gerarchico**, **molto ramificato**, **ricco** e **completo**. Esso permette di codificare tutti gli eventi che possono avvenire durante l’episodio clinico di un paziente e quindi si presta perfettamente per essere utilizzato nelle **cartelle cliniche informatizzate.**

1. **LOINC** – Logical Observation Identifiers Names and Codes: è un sistema di codifica standardizzato per la **descrizione univoca di osservazioni cliniche e di laboratorio**
   * + La storia: creato nel **1994** e mantenuto da **aggiornamenti semestrali** dal Regenstrief Institute, **ente di ricerca no profit associato all’Indiana University**. **Inizialmente** classificava principalmente le osservazioni effettuate ai **laboratori di analisi**, successivamente fu **espansa** per contenere anche: diagnosi infermieristiche, classificazione degli outcome, osservazioni relative a strumenti di prevenzione, diagnosi e cura dei pazienti
     + **Organizzazione**: è suddivisa in due parti principali:
       - **Laboratory LOINC**: test di laboratorio
       - **Clinical LOINC**: ampia varietà di rilevazioni esterne ai laboratori
       - Altre sezioni
         * Documenti clinici
         * Clinical report
         * Scala di valutazione del coma
         * Scala di valutazione della depressione
     + Un **termine** **LOINC** è definito dalla combinazione del **codice LOINC** e il **Fully Specified Name (FSN)**
     + Parametri dei codici LOINC
       - **Componente**
       - Tipo di **proprietà** misurata
       - Intervallo di **tempo** di misurazione
       - Il **sistema** o **l’oggetto** misurato
       - **Scala** di misurazione
       - **Metodo** di misurazione
     + La versione italiana è aggiornata semestralmente dal 2010
     + Il sistema è ad uso **gratuito**
     + È previsto che LOINC venga utilizzato all’interno del documento “**Referto di laboratorio**” per la valorizzazione dei campi: specialità dell’esame e risultato della misurazione
     + Consente di leggere e interpretare dati provenienti da sistemi differenti, identificando univocamente esami di laboratorio
     + Obiettivo del sistema è **codificare l’osservazione in sé, in modo standard ed univoco**, non tanto il valore che essa può assumere
     + L’elevato livello di **dettaglio** del sistema LOINC consente una **trasmissione precisa dei dati di laboratorio**, rendendo i risultati **comprensibili** e **riutilizzabili**, per i diversi provider di cura.
     + Si evita così la duplicazione di test ed esami
     + È un **database e uno standard universale** per l'identificazione delle osservazioni di laboratorio medico, disponibile pubblicamente
     + Assistere nello scambio elettronico e nella raccolta di risultati clinici
     + Diversi standard, come HL7, utilizzano LOINC per trasferire elettronicamente i risultati, da diversi sistemi di refertazione alle reti sanitarie appropriate.
2. **ATC** – Anatomical Therapeutic Chemical Classification System of Drugs: è un sistema internazionale di **codifica dei principi attivi dei farmaci**, anche veterinari, che si basa su caratteristiche **Anatomiche**, **Terapeutiche** e **Cliniche**. È controllata **dall’OMS**.
   * + Codifica: ogni codice è composto da **7 caratteri**, che servono a classificare il farmaco nei **5 livelli della classificazione**: **gruppo anatomico** principale, **gruppo terapeutico** principale, **sottogruppo terapeutico** farmacologico, **sottogruppo terapeutico/chimico**, **sottogruppo chimico**
     + Si possono **evitare errori** incrociando l’ATC o AIC con le allergie e le intolleranze del paziente.
     + Un **software** può segnalare possibili **incompatibilità** nell'uso contemporaneo di più farmaci su uno stesso paziente. È possibile fare **statistiche** e calcolo dei **costi** ed evitare usi impropri del farmaco
     + È **adatta** e **specifica** per le **necessità**
     + Il **numero dei caratteri** di ogni codice permette di classificare **milioni di farmaci diversi**
     + I **codici numerici** ed **alfanumerici in posizioni fisse** agevolano la **lettura** del codice e la posizione nella classificazione. Si dice che il codice è **parlante**
3. **AIC** – Autorizzazione all’Immissione in Commercio dei Farmaci: **identifica i farmaci in commercio in Italia**. È stampato sulle **fustelle** dei farmaci. Permette di distinguere ogni confezione farmaceutica non solo in base al **principio attivo,** ma anche dagli **eccipienti**, **numero di unità**, **via di somministrazione**. È rilasciato **dall’AIFA** che lavora in stretta collaborazione con EMA (agenzia comunitaria UE per la valutazione dei medicinali che ha sede ad Amsterdam)
4. Classificazione e codifica delle strutture sanitarie italiane: il **Nuovo Sistema Informativo Sanitario** (**NSIS**) prevede la classificazione e la **codifica delle strutture sanitarie utilizzando una serie di codici di tipo amministrativo.**

Standard di integrazione dei dati sanitari

**Norme tecniche**: sono **documenti che definiscono le caratteristiche di un prodotto, processo o servizio**

**Ente nazionale italiano di unificazione** (**UNI**): è **un’associazione privata** che elabora e pubblica **norme tecniche per tutti i settori.** Rappresenta l’Italia presso le **organizzazioni di normazione europea** (**CEN**) e **mondiale (ISO)**. Caratterizza tutte le norme nazionali italiane.

Sigle che identificano le norme tecniche

* **UNI** - sigla dell’Ente nazionale italiano di unificazione
* **EN** - sigla che identifica le norme elaborate dal CEN
* **ISO** - sigla che identifica le norme elaborate ISO

Standard “De jure” e “De facto”

* Uno standard, dal latino extendere, è un modello di riferimento utilizzato per uniformare le caratteristiche di un prodotto o di un servizio.
* L'obiettivo di uno standard è semplificare e migliorare i processi operativi, ottimizzare le risorse e ridurre i costi.
* Due tipologie:
  + Standard De Jure, definito in forza di una **legge**, cioè di una norma
  + Standard De Facto, imposto nella **pratica comune** per l’uso e per la grande diffusione

Esempi

* **PDF**/A: è uno standard **de jure** per l’archiviazione a lungo termine dei documenti. È **liberamente** e **gratuitamente** utilizzabile
* **DOCX** di Microsoft Word: è uno standard **de facto** per videoscrittura, protetto da **copyright** (a **pagamento**)

Vantaggi:

* Condivisione di una **sintassi**
* Condivisione di una **semantica**
* Riduzione dei **costi**
* Ciò permette di fare **interagire con efficienza i sistemi informatici**, indipendentemente da marca e modello.

1. L’associazione HL7: **Health Level 7** è l’associazione internazionale di tipo **no profit** che gestisce alcuni **importanti standard in ambito sanitario**, tra cui il **linguaggio** **HL7**. È stata fondata nel **1987** e riunisce **organizzazioni affiliate in oltre 40 paesi**. Non sviluppa software, non ha fini di lucro, bensì **fornisce le specifiche tecniche di alcuni standard sanitari e ne promuove l’uso**. HL7 è un **linguaggio standard per lo scambio**, la **gestione** e **l’integrazione** dei **dati**, che supportano la fase di cura del paziente e per la gestione, l’erogazione e la valutazione dei servizi sanitari. Il **livello 7** è quello **applicativo** caratterizzato dall’uso di un **linguaggio quanto più possibile vicino all’uomo, cioè comprensibile ed intellegibile**
   * Versioni:
     + **v2** usa messaggi di **testo** in formato **ASCII**: ha un’impostazione **message oriented**, i dati sono scambiati tramite messaggi, è **posizionale**
       - Ogni messaggio è composto da uno o più **segmenti**, il primo è detto **message** **header segment** (MSH), ogni segmento è identificato da tre lettere poste al suo inizio (**intestazione**) ed è formato da sequenze di **campi**. I segmenti sono separati tra loro mandando **a capo** la riga. I campi possono essere obbligatori, opzionali, ripetuti, di lunghezza fissa o variabile. I campi sono separati da simboli di **pipe** e possono essere a loro volta essere suddivisi in **sottocampi** separati da **apice** o **e commerciale**
       - Tipi di messaggi
         * **ACK** – General acknowledgement
         * L’HL7 utilizza un messaggio di Acknowledgement per **garantire la sicurezza nel trasferimento dei messaggi.**
         * Quando un messaggio viene inviato da un attore A ad un attore B, l’attore A attende che l’attore B invii un messaggio di Acknowledgment (ACK) per essere sicuro che il messaggio sia stato ricevuto correttamente.
         * I dati generati da un elettromedicale, vengono cancellati dallo stesso solo quando quest’ultimo è sicuro che siano salvati su un server. Così l’esame non si «perde».
         * Negative ACK

Il messaggio Negative Acknowledgments (NACK), permette al mittente di sapere che c’è stato un errore nel processamento del messaggio

* + - * + ADT –Admit, Discharge, Transfer
        + **ORU** –Observation result (unsolicited)

**trasmette** **osservazioni e risultati dal sistema produttore al sistema di ordinazione/collocatore**

Può anche essere utilizzato per:

trasmettere i dati dei risultati **dal sistema di produzione a un sistema di archiviazione** di cartelle cliniche o a un altro sistema che non fa parte del processo di ordinazione originale.

per registrarsi o collegarsi a studi clinici o per scopi di refertazione medica per farmaci e dispositivi.

I tipi di osservazioni riportati nel messaggio ORU-R01 includono:

Risultati di laboratorio clinico

Rapporti di studio di imaging (non trasporta le immagini)

Risultati dello studio funzionale

Condizione del paziente o altri dati (ad es. segni vitali, sintomi, allergie, note, ecc.)

II messaggi ORU **non contengono immagini**; usano diversi tipi di dati ma molto spesso usano testo, numeri e codici.

* + - * + **Z-Segment**

L'HL7 v2.x standard contempla circa **140 segmenti standard**.

L'HL7 v2 **prevede l'uso di segmenti non standard, che iniziano con la lettera Z.**

Uno Z- segment è un **messaggio definito localmente** e non fa parte dei messaggi HL7 standard.

Gli Z-segments sono uno dei motivi per i quali l'HL7 v2 è considerato uno **standard flessibile.**

Punti favorevoli:

Rendono il linguaggio HL7 molto flessibile;

Sono semplici da usare

Punti sfavorevoli:

Rendono il linguaggio HL7 poco standard

* + - **v3** usa messaggi in formato **XML**: è uno standard **de jure,** è **object oriented,** ed utilizza un **modello di riferimento** chiamato **RIM** che fornisce una **rappresentazione** di persone, enti, ruoli, partecipazioni ed atti delle classi e del dominio clinico; identifica il **ciclo di vita dei messaggi, le relazioni tra essi e gli eventi scatenanti**, definisce i **templates** e un **vocabolario** per assegnare una **semantica univoca** ai dati contenuti nei messaggi. È uno standard **maturo**
      * utilizza un **modello di riferimento** (RIM), **vieta l’uso degli Z segment**, è più formale, **non è più posizionale ma utilizza dei tag** (metadati)

**World Wide Web Consortium**: è **un’organizzazione non governativa internazionale** che ha come scopo quello di favorire lo sviluppo di tutte le potenzialità del world wide web e diffondere la cultura dell’accessibilità della rete. La sua principale attività consiste nello stabilire **standard tecnici per il world wide web** inerenti sia a linguaggi di markup che a protocolli di comunicazione. In particolare, ha definito:

* **Modello dei dati RDF**:
  + **Risorsa**: indica ciò che viene descritto mediante questo modello, può essere sia interna che esterna al web
  + **Proprietà**: indica un attributo o una relazione utilizzata per descrivere una risorsa. Il suo significato e le sue caratteristiche vengono definite tramite lo schema RDF
  + **Espressione**: è l’elemento che descrive la risorsa, costituito da: soggetto, predicato, oggetto
* **JSON** – **Java Script Object Notation**: è un **formato file aperto** adatto **all’interscambio di dati fra applicazioni client-server:** **semplicità** di utilizzo, sia **machine readable che human readable**, grazie all’utilizzo di **chiavi (metadati)** edi **valori**

**API** – Application Programmi Interface: indica un insieme di **definizioni** e **protocolli** per la **creazione e l’integrazione di applicazioni software**. **Permettono a prodotti o servizi di comunicare tra loro** senza conoscere come questi sono stati implementati. Garantiscono **flessibilità**, **semplificando** così **progettazione**, **amministrazione** e **utilizzo** offrendo inoltre opportunità di innovazione.

* Sicurezza: le API consentono **l’accesso alle risorse aziendali** mantenendo **sicurezza** e **controllo**. È l’azienda a decidere come e a chi concedere l’accesso. Api danneggiate, esposte o oggetto di attacchi informatici sono la causa di gravi violazioni di dati. La maggior parte delle implementazioni di API si divide
  + **REST**: utilizzano il protocollo **http** e supportano la **crittografia TLS**, standard che consente di **mantenere privata una connessione** internet e controlla che i **dati** inviati siano **crittografati** e **non modificati**. Usano **JSON**, un formato file che semplifica il trasferimento dei dati tramite browser web
  + **SOAP**: utilizzano **WS Security**, protocolli integrati che definiscono un **set di regole** basato sulla **riservatezza** e **sull’autenticazione**. Tali set di regole sono definiti dai due principali organismi di normalizzazione internazionali: **OASIS** e **W3C**. Come **protocolli** di **sicurezza** utilizzano una **combinazione di crittografia XML, firme XML e token SAML**, a tale maggior livello di sicurezza corrisponde un maggior livello di **complessità gestionale**

HL7 versione FHIR: è uno standard per lo scambio di informazioni mediche, descrive i formati dei dati medici e lo scambio di questi attraverso l’API REST. È su v2 e v3 di HL7 ma più semplice nell’implementazione

**CDA – clinical document architecture**: è un **linguaggio nato nell’ambito di HL7**, basato sullo standard **XML** che ha l’obiettivo di **specificare la codifica, la struttura e la semantica di un documento clinico**. Può contenere qualsiasi tipo di contenuto clinico. Specifica la **sintassi** e la **semantica** di un documento clinico. Caratteristiche: **persistenza**, **controllo**, possibilità di **autenticazione**, **contesto**, **integrità**, **leggibilità umana**. È stato sviluppato utilizzando **HL7 v3,** specifica che il contenuto del documento è costituito da:

* **Parte testuale obbligatoria**: per **l’interpretazione umana** del contenuto del documento
* **Parti strutturate facoltative**: per **l’elaborazione del software**, basata su sistemi di codifica come **SNOMED** e **LOINC** per rappresentare i concetti

1. **DICOM** – Digital Imaging and Communication in Medicine: è uno standard per la **generazione**, **l’archiviazione**, la **visualizzazione**, la **stampa** e la **trasmissione** delle **immagini mediche** e delle **informazioni ad esse associate**. È pubblico e consente di avere una base di interscambio fra apparecchiature di diversi produttori, server e PC, specifica per l’ambito biomedico. Ha permesso di ottenere **compatibilità tra diversi strumenti e fornitori**, migliorando **efficienza** e **interoperabilità** negli ambienti sanitari. **HL7 e DICOM si completano l’un l’altro**. Per leggere un file DICOM serve un **visualizzatore**, i messaggi HL7 sono facilmente leggibili dall’uomo.

* Storia: con l’introduzione di **modalità di imaging diagnostico digitale negli anni 70** sorge il problema di creare uno standard per il trasferimento di immagini e informazioni associate tra dispositivi. ACR e NEMA formano un comitato congiunto creando lo standard **ACR-NEMA**, la cui versione **3.0** prende il nome di **DICOM**.
* **Conformance statement**: **la compatibilità di qualsiasi dispositivo allo standard DICOM** deve essere certificata dal costruttore attraverso un documento denominato Conformance Statement, che ne elenchi le **funzionalità**. Il buon esito di una connessione tra due apparecchiature DICOM è in prima istanza legato a questo.
* Principi:
  + **Applicabilità globale e localizzazione**: è uno standard globale che si adatta ai requisiti culturali e alle politiche sanitarie locali senza deviare dallo standard
  + **Manutenzione continua**: più volte all’anno, uno dei requisiti dell’aggiornamento dello standard è di mantenere l’effettiva compatibilità con le edizioni precedenti
  + **Oggetti informativi e identificazione univoca dell’oggetto**: molti servizi DICOM comportano lo scambio di **oggetti informativi persistenti**, come le **immagini**. **Un'istanza** di tale oggetto informativo può essere scambiata attraverso molti sistemi e molti contesti organizzativi e nel tempo. Sebbene possano essere apportate modifiche minori agli attributi di un’istanza, il suo **contenuto semantico** non cambia e questa è identificata da un **identificatore di oggetto** **univoco globale**. Modifiche al contenuto semantico creano una nuova istanza.
    - **Definizione**, **descrizione del suo scopo** e **attributi** che li definiscono. Due classi: **normalizzati**, **composti**
  + **Conformità**: la conformità allo standard è definita in base ad una serie di **classi SOP**, le cui specifiche sono modificate in modo da essere compatibili con tutte le versioni per tutte le edizioni dello standard
  + **Coerenza del modello informativo**: un gran numero di Information Objects definiti nello standard DICOM segue un modello informativo comune con entità informative che rappresentano una **semplificazione dei concetti e delle attività del mondo reale dell’imaging medico.** Tale modello semplificato è sufficiente per le esigenze pragmatiche di gestione dell’imaging. **I nuovi oggetti saranno generalmente conformi a questo modello di informazioni.**

**IHE** – Integrating the Healthcare Enterprise: è **un’iniziativa degli operatori sanitari e dell’industria** per **migliorare il modo in cui i sistemi informatici nel settore sanitario condividono le informazioni.** Promuove **l’uso coordinato di standard consolidati** come DICOM e HL7 per soddisfare esigenze cliniche specifiche a supporto di un’assistenza ottimale al paziente. I sistemi sviluppati in conformità con IHE **comunicano meglio tra loro**, sono **più facilmente implementabili** e consentono un **utilizzo più efficace delle informazioni.**

* + Obiettivi:
    - assicurare che tutte le informazioni richieste per le decisioni cliniche siano corrette e facilmente reperibili da parte delle varie figure professionali coinvolte.
    - definire in maniera chiara come gli standard esistenti devono essere utilizzati
  + "**Profili IHE**", sono pubblicati, non sono imposti ma definiti in modo cooperativo da un campione rappresentativo di interessati

FSE- Fascicolo Sanitario Elettronico

È l’insieme dei **dati** e dei **documenti** **digitali** di tipo **sanitario e sociosanitario**, generati da **eventi clinici** presenti e trascorsi, che riguardano l’assistito.

Il fascicolo copre **l’intera vita del paziente**, dalla nascita alla morte.

La cartella clinica contiene le informazioni relative ad un singolo episodio clinico, un solo ricovero. Il FSE contiene le informazioni di tutta una vita

È istituito dalle **regioni** e **province autonome**, nel rispetto della normativa vigente in materia di **protezione dei dati personali**, a fini di:

* prevenzione, diagnosi, cura e riabilitazione;
* studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;
* programmazione sanitaria, verifica delle qualità delle cure e valutazione dell’assistenza sanitaria.

È suddiviso in:

* **Nucleo minimo di dati e documenti** (obbligatori): dati identificativi ed amministrativi, profilo sanitario sintetico, dossier farmaceutico, consenso o diniego alla donazione di organi e tessuti
* **Dati e documenti integrativi**, che permettono di arricchire il fascicolo (facoltativo): taccuino personale

Il FSE è un **oggetto unico**

Il fascicolo appare come un unico oggetto, anche se in realtà è una collezioni di **informazioni fisicamente** **“distribuite” su più banche dati regionali**. Il FSE raccoglie e rende disponibili tutti i documenti sociosanitari generati dalle strutture cliniche all’atto dei rapporti dei pazienti con i diversi attori del SSN. Ciò facilità il **reperimento**, la **conservazione** e la **gestione** dei documenti per gli utenti ed i professionisti della sanità, ovunque essi si trovino ed in qualunque momento.

È alimentato in maniera continuativa

Consenso e revoca

Consultazione dei dati

Tutte le **informazioni** del FSE viaggiano in rete in modalità **criptata** e sono invisibili agli hacker

Codifiche dei dati e standard documentali

* HL7 per descrivere le definizioni dei dati da scambiare
* CDA
* ICD9-CM
* LOINC
* AIC
* ATC

L’Infrastruttura Nazionale per l'Interoperabilità ha il compito di:

1. Garantire **l’interoperabilità** dei FSE regionali;
2. Garantire **l’identificazione dell’assistito** attraverso l’allineamento con **l’Anagrafe Nazionale degli Assistiti (ANA);**
3. Garantire **l’interconnessione dei soggetti** previsti per la trasmissione telematica dei dati per le regioni;
4. Garantire la **gestione delle codifiche nazionali e regionali**.

Architettura

* **Archivio**, detto Repository
* **Indice** dei dati archiviati, detto Registry (indice): contiene i **metadati**, informazioni sul documento sanitario generato
* Una **porta di accesso alla rete dati**, detto Gateway: sistema che si occupa di raccogliere, aggregare e formattare il FSE. È **distribuito**, **stateless** ed il **punto di accesso dei client all’infrastruttura di base**. Garantisce la visibilità del fascicolo attraverso internet

Vantaggi

* Permette ad un **operatore sanitario di inquadrare un paziente a lui sconosciuto** durante il contatto in emergenza/urgenza;
* Rende disponibile la **storia clinica** del paziente
* Permetta a diversi operatori che hanno già in carico un paziente di essere consapevoli delle iniziative diagnostiche e terapeutiche portate avanti dai **colleghi**
* Permette di **condividere tra gli operatori le informazioni amministrative od organizzative/ausiliarie**
* Controllo della **spesa sanitaria**

Presupposti

* Utilizzo di **linguaggi standard**
* Utilizzo di **codifiche univoche**
* Utilizzo di **codici identificativi univoci per le strutture sanitarie** pubbliche e private, per i **reparti** e per i **documenti**
* Un’**anagrafe centrale** idonea ad identificare univocamente ogni paziente
* Una **rete dati a banda larga**

Principali modalità di utilizzo:

* **Primario**: a diretto vantaggio della salute del paziente
* **Secondario**: a vantaggio indiretto per il paziente

I documenti sono suddivisi in tre sezioni: **sanitari**, **amministrativi** e **prescrizioni**

**Normalizzazione**

* È un procedimento che a partire da uno **schema relazionale non normalizzato**, permette di ottenere uno **schema relazionale normalizzato**
* Non è una metodologia di progettazione, bensì uno **strumento di verifica**
* **La metodologia di progettazione basata su schemi ER produce normalmente schemi relazionali normalizzati**
* Le verifiche di normalizzazione possono essere applicate anche agli schemi ER
* Spesso si incorre in problematiche causate dalla rappresentazione in maniera scorretta delle dipendenze all’interno di tabelle
  + **Ridondanza**
  + **Anomalia di aggiornamento** (se una dipendenza è ripetuta, in caso di aggiornamento di quel dato, si dovranno modificare singolarmente tutte le ennuple che lo contengono)
  + **Anomalia di inserimento** (non può essere inserito un nuovo dato che non contenga tutti i campi, es. uno studente che non abbia sostenuto esami)
  + **Anomalia di cancellazione** (es. cancellando gli esami si cancella anche lo studente)
* Tali problemi sorgono perché vi è un tentativo di rappresentare **informazioni eterogenee**
  + Alcuni dati sono ripetuti in tuple diverse senza aggiungere nuova informazione 🡪 **dati ridondanti**
  + **Le** **informazioni ridondanti devono essere aggiornate in modo atomico** (tutte contemporaneamente)
  + **La cancellazione di una tupla comporta la cancellazione di tutti i concetti da essa rappresentati, inclusi quelli che potrebbero essere ancora validi**
  + **L’inserimento di una nuova tupla è possibile solo se esiste almeno l’informazione completa relativa alla chiave primaria**, non è possibile inserire la parte di tupla relativa ad un solo concetto

**Forma normale di Boyce Codd**

* È basata sul **concetto di dipendenza funzionale**
  + È un particolare tipo di **vincolo di integrità**
  + Descrive **legami di tipo funzionale tra gli attributi di una relazione**
  + Es. matricola dello studente implica/determina/seleziona in modo univoco residenza, nome, cognome, dataN
  + Una **relazione soddisfa la dipendenza funzionale** **X🡪Y** (X e Y = insiemi di attributi; 🡪 = implica) se, prese **due tuple qualsiasi** della relazione di nostro interesse (tabella), che hanno **gli stessi attributi in X**, queste abbiano **gli stessi attributi anche in Y**
  + **Qualunque chiave K di una relazione ha la proprietà di determinare tutti gli altri attributi**
  + Siamo interessati a **dipendenze funzionali non banali**: dipendenze funzionali che **non contengono lo stesso attributo da tutti e due i lati della dipendenza** (es. di dipendenza banale: matrstudente codcorso 🡪 codcorso)
* Le **anomalie** sono causate da **proprietà degli attributi coinvolti in dipendenze funzionali**
* **Le** **dipendenze funzionali dalle chiavi non originano anomalie, quindi se si riuscisse ad ottenere dipendenze funzionali solo di chiave non si avrebbero anomalie**
* Le anomalie sono causate
  + **Dall’inclusione di concetti indipendenti tra loro nella stessa relazione**
  + Da **dipendenze funzionali** X🡪Y che permettono la **presenza di più tuple con lo stesso valore di X**: X non contiene una chiave, **il fatto che un attributo in X** possa essere ripetuto genera ridondanze e dimostra che esso **non è una chiave**
* Una relazione è in **BCNF** se, **per ogni dipendenza funzionale (non banale)** X🡪Y definita su di essa, **X contiene una chiave di r** (X è **superchiave** di r)
* In relazioni BCNF non sono presenti anomalie e ridondanze perché **concetti indipendenti sono separati in relazioni diverse**
* **Decomposizione** BCNF
  + Normalizzazione
    - **Processo di sostituzione di una relazione non normalizzata con due o più relazioni in BCNF**
  + **Criterio**
    - Una relazione che rappresenta più concetti indipendenti è decomposta in relazioni più piccole, una per ogni concetto, per mezzo delle dipendenze funzionali
  + Le nuove relazioni sono ottenute mediante **proiezioni** (π) **sugli insiemi di** **attributi corrispondenti alle dipendenze funzionali**
  + Le **chiavi delle nuove relazioni sono le parti sinistre delle dipendenze funzionali**
    - Le nuove relazioni sono in BCNF
  + **Proprietà** della decomposizione
    - Problematiche
      * **Perdita di informazione**
        + **Decomposizione senza perdita:** garantisce che le informazioni nella relazione originaria siano **ricostruibili con precisione** (senza **tuple spurie**) a partire da quelle nelle relazioni decomposte
      * **Perdita delle dipendenze**
        + **Conservazione delle dipendenze**: garantisce che le **relazioni decomposte abbiano la stessa capacità della relazione originaria di rappresentare i vincoli di integrità**
    - Data la relazione **r(X)** e gli **insiemi di attributi X1 e X2** tali che
      * **X = X1 u X2**
      * **X0 = X1 ∩ X2**

Se **r** soddisfa la **dipendenza funzionale**

* X0 🡪 X1 o X0🡪X2

La decomposizione di r su X1 e X2 è **senza perdita**

* + - **Gli attributi comuni formano una chiave per almeno una delle relazioni composte**

**Terza forma normale**: o **X è superchiave** o **ogni elemento di Y fa parte di una chiave**