AIIC 2025 CONVEGNO NAZIONALE ASSOCIAZIONE ITALIANA INGEGNERI CLINICI

NAPOLI 14-17 GIUGNO 2025 MOSTRA D'OLTREMARE

AIIC associazione italiana ingegneri clinici

SALE OPERATORIE INTEGRATE: STATO DELL'ARTE E PROSPETTIVE FUTURE TRA TECNOLOGIE, DATI E PROCESSI

Dati, interoperabilità e sicurezza

Alberto Lombardi
Direttore UOC Ingegneria Clinica HTA
Telemedicina ed Evoluzione Digitale

Contatti alberto.lombardi@aslbenevento.it

RELATORI

TECNOLOGIE, SOSTENIBILITÀ, AMBIENTE
Il contributo dell'innovazione alla sanità del futuro

Di cosa parleremo?

- Introduzione
- Flusso e Gestione dei Dati Clinici
- Integrazione dei dati con cartella clinica e sistemi informativi ospedalieri
- Standard di Comunicazione e Interoperabilità
- Interoperabilità tra dispositivi multi-brand
- Cybersecurity in ambito clinico
- Applicazione del GDPR alla sanità digitale

Introduzione

Gestione sicura, interoperabile ed efficiente delle informazioni sanitarie.

→

Reti IT medicali - Applicazione della normativa GDPR e dei framework regolatori europei (NIS2, MDR);

→

Sicurezza informatica (cybersecurity) nei sistemi digitali clinici;

↓

Integrazione dei dati con la cartella clinica elettronica (CCE) e i sistemi informativi ospedalieri (SIO);

→

Standard di comunicazione e interoperabilità tra dispositivi clinici eterogenei;

→

Obiettivo:

migliorare la qualità delle cure, supportare la continuità assistenziale e alimentare sistemi di decisione clinica automatizzata.

Rete IT Medicali

Definizione di rete IT medicale

Una **rete IT medicale** è un'infrastruttura informatica progettata per connettere dispositivi medici, sistemi informativi clinici e applicazioni sanitarie all'interno di un ambiente ospedaliero o sanitario. Il suo scopo è garantire l'interoperabilità, la sicurezza dei dati e la continuità operativa nei processi clinici.

CARATTERISTICHE DISTINTIVE RETE IT_DM

- **Connessione di dispositivi medici (IoMT)**: come monitor multiparametrici, pompe infusionali, ventilatori, ecc.
- **Gestione del rischio**: secondo la norma IEC 80001-1, che integra aspetti di safety, security e privacy.
- **Segmentazione della rete**: tramite VLAN dedicate per isolare i dispositivi medicali da altri sistemi.
- **Protezione dei dati sensibili**: in conformità con il GDPR e le normative europee sui dispositivi medici (MDR 2017/745).
- **Contromisure tecniche**: come whitelisting, TLS, logging centralizzato, IDS e aggiornamenti firmware.

Integrazione competenze IT - IC

L'evoluzione ha portato a dover integrare in un unico processo professionalità fino a pochi anni fa completamente autonome, con evidenti difficoltà nell'amalgamare ruoli e competenze tradizionalmente focalizzate su problematiche e approcci distinti.
Tale integrazione è oramai indispensabile e "obbligatoria".

Ingegnere Clinico

Principali "Skill culturale" e "sensibilità professionale" :

- Elettronica, elettrotecnica, meccanica, chimica, fisiologia: principi fisici di funzionamento dei dispositivi medici (apparecchi, strumentazione, tecnologie)

- DM e gestione del rischio, in particolare safety

- Valutazione e acquisizione tecnologie DM

Esperto IT

Principali "Skill culturale" e "sensibilità professionale" :

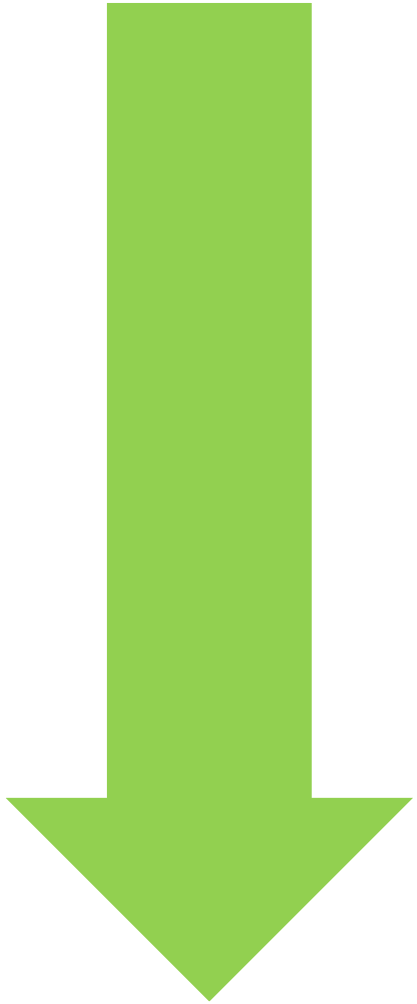
- Elettronica, informatica e telecomunicazioni: principi alla base delle tecnologie dell'informazione e della comunicazione (ICT)

- Gestione del rischio, in particolare data and system security e privacy

- Valutazione e acquisizione tecnologie IT

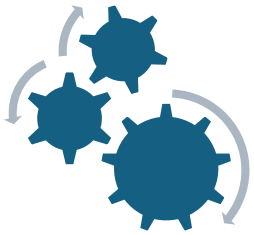
Integrazioni RETE IT – DM … il percorso

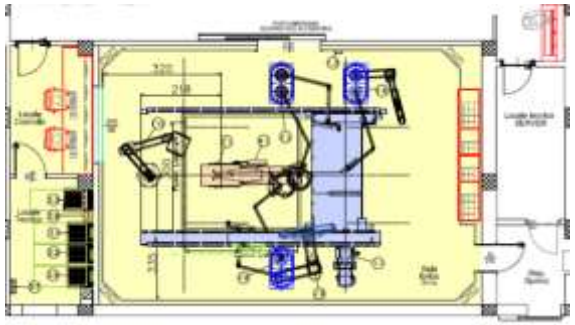
- Mappare i flussi informativi e il trattamento dati
- Definizione del Modello Architetturale tecnico e Organizzativo
- Progettazione dei sistemi in base modelli che garantiscono la protezione dati by default e by design
- Implementare un' architettura IT basata su standard di integrazione e principi di interoperabilità
- Adottare di Strumenti di security e safety integrati
- Adottare Strumenti di valutazione e riduzione del rischio
- Adottare di Misure organizzative e tecniche



- Non perdersi nel labirinto degli
- Avere una visione sistemica di insieme
- Cogliere le opportunità con un approccio

Integrazione Dispositivi Medici e infrastruttura IT
Aspetti da attenzionare





Safety (E.M.)

Regolamento UE 2017/745 - DM
Art.71 D.Lgs. 81/08
Norma UNI 14971:12
Norma CEI EN 62353

Security (ICT)

Regolamento UE 2016/679 - GDPR
Norma CEI 62-237
Norma ISO 27001:13

Sicurezza DM-IT

Norma UNI ISO 80001-1

GDPR – Il nuovo approccio :
Accountability e gestione del rischio

Art. 32: Il titolare deve adottare **opportune misure** e per **dimostrare** la conformità per quanto riguarda **l'individuazione del rischio** connesso al trattamento, la sua **valutazione** in termini di origine, natura, probabilità e gravità, e l'individuazione di **migliori prassi per attenuare il rischio**

INDICAZIONI DEL DPO

LINEE GUIDA DEL GARANTE e del WP

CODICI DI CONDOTTA
CERTIFICAZIONI

Dalla forma alla sostanza: Il nuovo approccio basato sul rischio

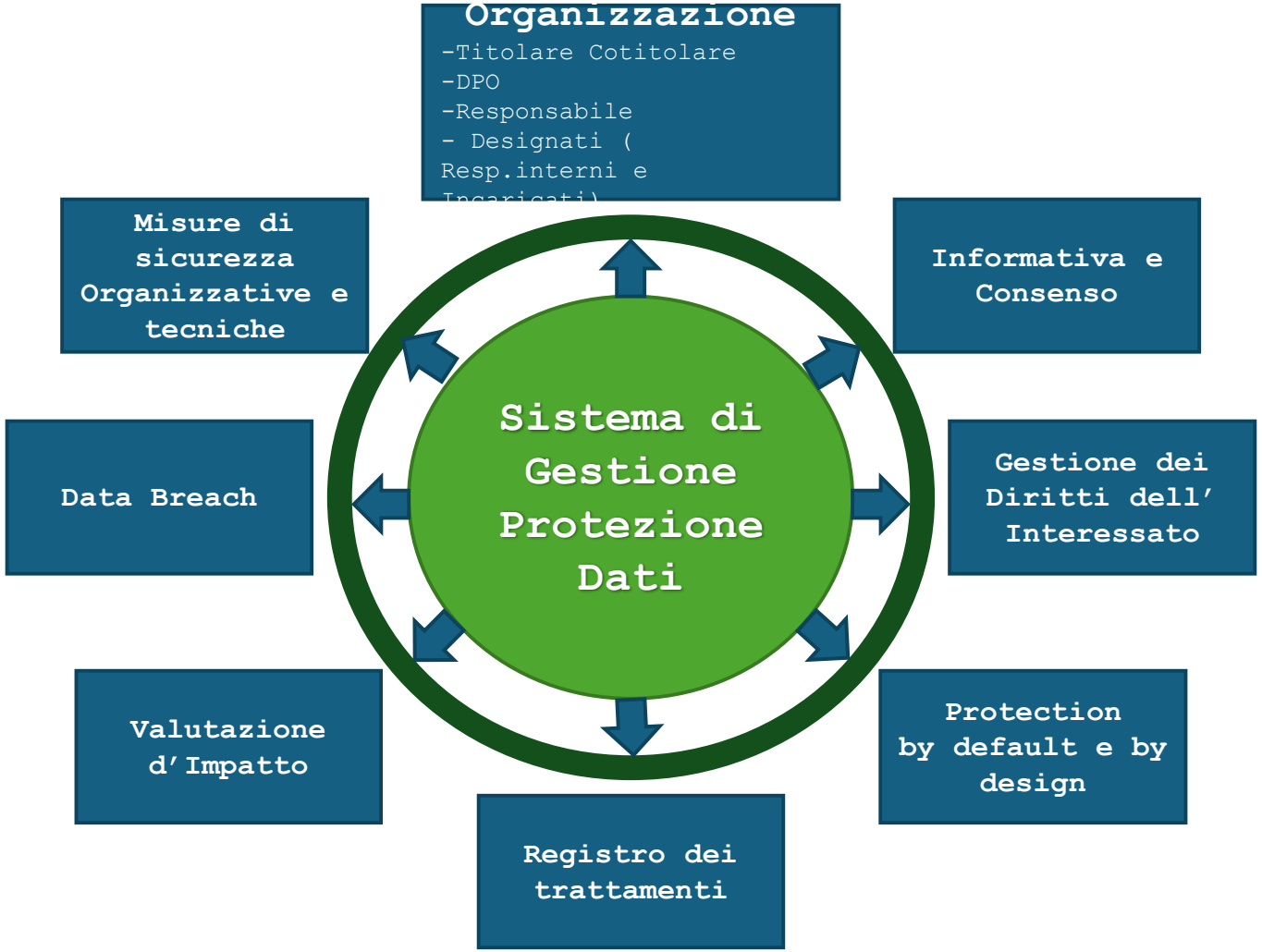
Art. 5.2: "Il titolare del trattamento è competente per il rispetto" dei principi applicabili al trattamento".. e in grado di comprovarlo"

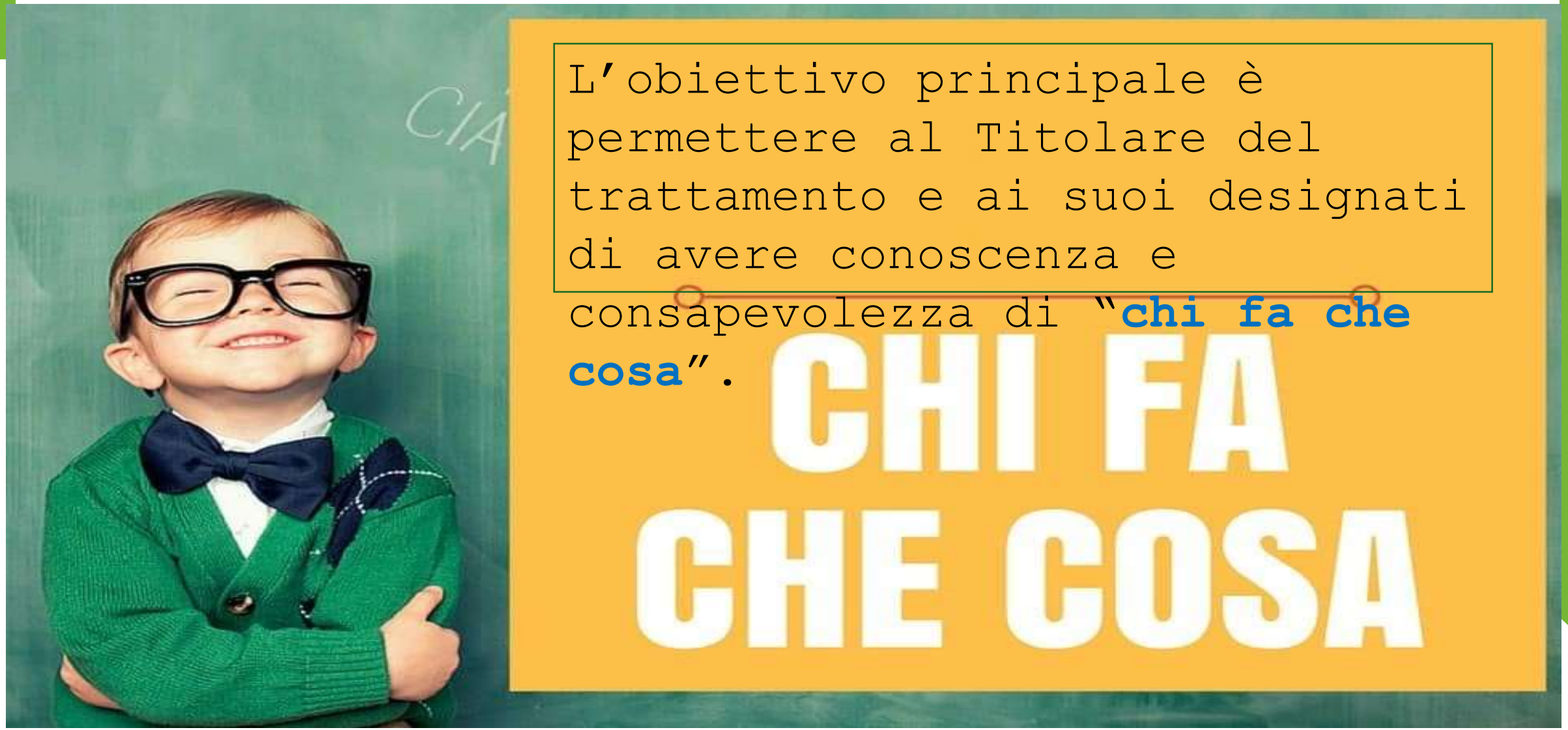
Cons. 74: (…il titolare del trattamento dovrebbe mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure

Art. 24 - 1: «Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformement regolamento.»

- **Conoscenza dei processi aziendali, dei flussi informativi e relativi trattamenti**
- **Individuazione, Valutazione e Gestione dei Rischi**
- **Adozione delle adeguate misure di sicurezza organizzative e tecniche**

Sistema di gestione della Protezione Dati





L'obiettivo principale è permettere al Titolare del trattamento e ai suoi designati di avere conoscenza e consapevolezza di "**chi fa che cosa**".

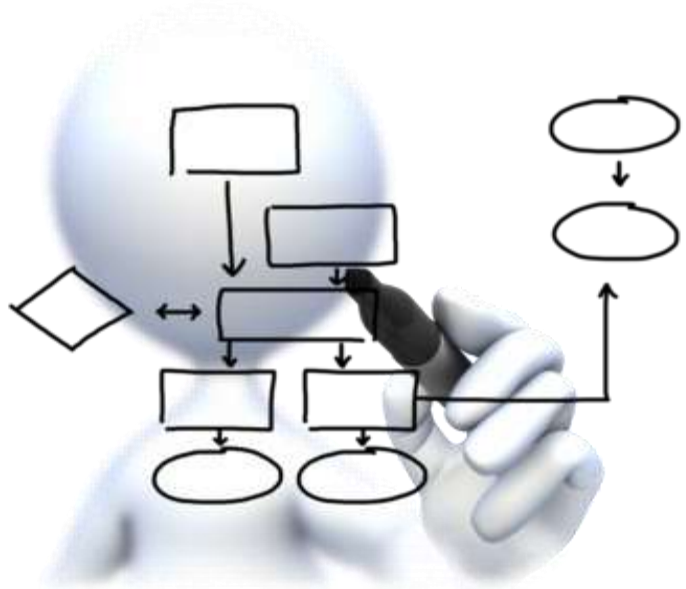
Mappatura dei processi e analisi dei flussi informativi

L'analisi ed individuazione dei trattamenti **deve essere** effettuata nella azienda attraverso un'attenta **mappatura dei processi** e quindi **analisi dei flussi informativi** ad esso sottesi

Anche se i processi sono vitali per un'organizzazione perché sono il modo in cui essa realizza i suoi obiettivi e implementa le sue strategie, difficilmente ***le aziende ne sono veramente consapevoli****.*

Manca ***la consapevolezza di cosa si fa in azienda e di come lo si fa****: Le attività e le procedure sono spesso* ***nella mente delle persone****.*

Questo porta con sé enormi rischi. Ad esempio il pensionamento di qualche figura cardine può provocare periodi di fermo o il rischio di ripartire con difficoltà dopo che si sono verificati problemi.



Mappatura dei processi e analisi dei flussi informativi

La mappatura dei processi e dei propri flussi informativi è composta dalle seguenti fasi fondamentali:

1. Identificazione delle **attività svolte**, e descrizione della situazione di "cosa avviene" nell'azienda.

2. Definizione, per ogni processo individuato, di **flussi informativi** e della **natura qualitativa e quantitativa dei dati trattati**.

3. Identificazione **e classificazione della tipologia di dati trattati**, in particolare l'identificazione di dati sensibili, ultrasensibili e giudiziari.

4. Identificazione e descrizione delle **modalità in** [illegible] **ed archiviato**.

Mappatura dei processi e analisi dei flussi informativi

5. Descrizione delle **articolazione aziendali**, delle **società esterne** o dei professionisti che **intervengono nel trattamento** con identificazione dei Responsabili esterni ed interni e di tutti gli attori che intervengono nel processo analizzato.

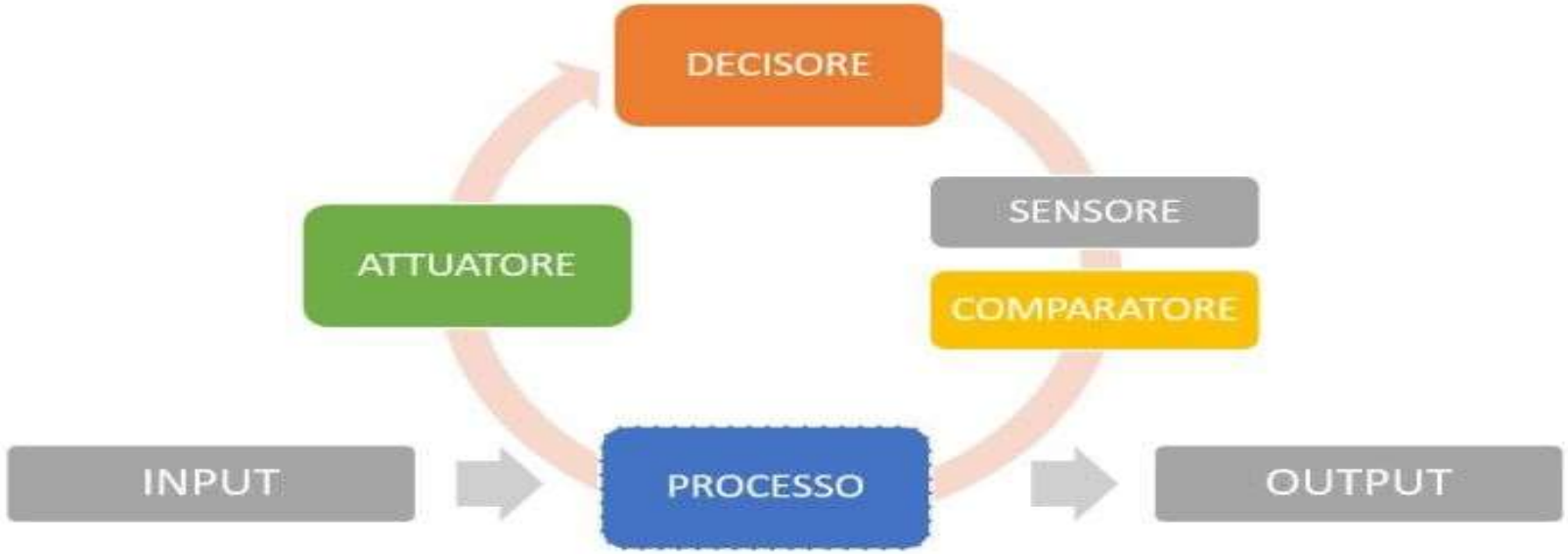
6. Identificazione dei **legami logici e delle interazioni con altri processi** e con ulteriori *attori* che intervengono nel trattamento a cui sono comunicati/trasmessi i dati.

7. **Semplificazione ed ottimizzazione dei processi**, cercando ridurre al minimo le informazioni utilizzate nel processo e il trattamento da effettuare sugli stessi (Protection by default e by design).

Mappatura dei processi e analisi dei flussi informativi

8. Individuazione e descrizione delle **misure organizzative e tecniche** utilizzate per garantire la sicurezza del trattamento con particolare riferimento alla trasmissione e all'archiviazione dei dati personali

9. Creazione di un **sistema in grado di monitorare i processi, i flussi informativi** e le tipologia di dati trattati al fine di apportare modifiche e miglioramenti ed adottare eventuali azioni correttive e preventive per garantire la sicurez



GDPR – Il nuovo approccio : I rischi del trattamento dei dati

Il nuovo regolamento generale ha un approccio basato sulla **valutazione del rischio (risk based)**, piuttosto che sulla protezione dell'utente.

Con tale valutazione si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto **della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti**.

Quindi, il rischio inerente al trattamento è da intendersi come l'impatto negativo sulle libertà e i diritti degli interessati.

Un "**rischio**" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.

La "**gestione dei rischi**", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi

Processo di valutazione dei rischi

Misure tecniche ed organizzative

Art. 32 GDPR

- Ridefinizione del **Modello Organizzativo**
- Creare **consapevolezza** con **informazione e formazione**
- Supporto e facilitazione **all'esercizio del diritti**
- Protezione **by default e by design**
- Sistema di **protezione e reazione alle violazioni**
- Strumenti di **valutazione e riduzione del rischio**
- Strumenti di **verifica e controllo conformità**

Mappatura dei processi e dei flussi,
Valutazione Rischio e Impatto,
Contratti con Responsabili,
Procedure
Formazione
Gestione archivi cartacei

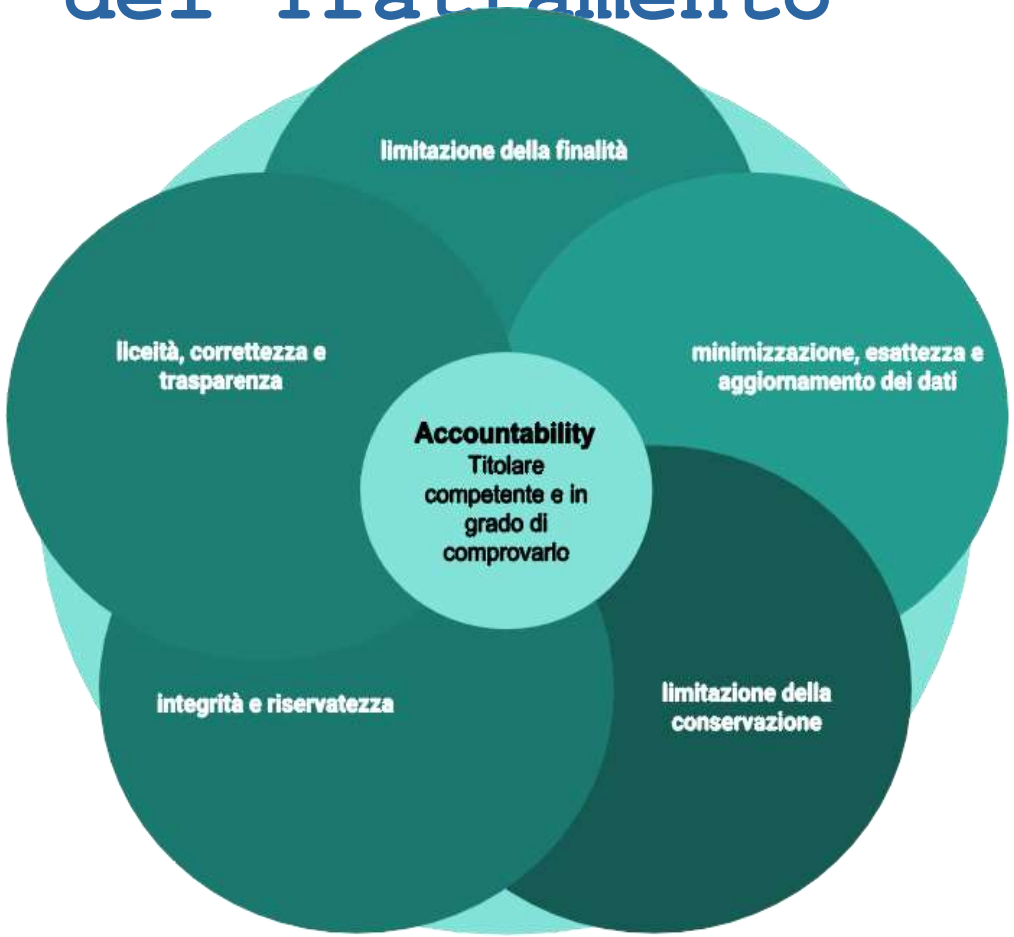
Misure Organizzative

Attuazione e GDPR

Misure [illegible] archivio
Cybersecurity
Credenziali,
Autorizzazione,
Cifratura
Pseudonimizzaizone,
Protezione perimetrale IT,
Businness Continuity
Disaster Ricovery

Misure Tecniche

L' Accountability garanzia dei principi del Trattamento



Principi del trattamento

- **Liceità** : I dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

- **Finalità:** I dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

- **Minimizzazione ed Esattezza:** I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati - Esatti e, se necessario, aggiornati

- **Limiti di conservazione:** I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati

- **Riservatezza ed integrità:** I dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate

Violazione dei dati personali - Data Breach

Violazione dei dati personali (c.d. Data breach) è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, punto 12 - GDPR).

Possibile cause di violazione:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

Data Breach – Gli Obblighi del Titolare

Il titolare deve:

o **Notificare** la violazione all'autorità di controllo **senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui ne è venuto a conoscenza, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti** e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

o **Documenta** qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue **conseguenze** e **i provvedimenti adottati per porvi rimedio**

o **Comunica la violazione all'interessato senza ingiustificato** ritardo, quando la violazione dei dati personali **è suscettibile di presentare un rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento (non obbligatoria se **intraprese misure** - pre o post violazione- adeguate a **contenere il rischio non elevato** oppure **sforzi sproporzionati**)

Data Breach – Fasi del processo di gestione

La gestire di una violazione dei dati personali è stata standardizzata in un processo suddiviso nelle seguenti quattro fasi:

1 - Identificazione e indagine preliminare: A seguito di ricezione della segnalazione da parte di uno degli attori, il Titolare del trattamento, per il tramite del Responsabile Ufficio Privacy effettua la registrazione e l'identificazione univoca della segnalazione, quindi, con il supporto del Responsabile della Protezione Dati, effettua una valutazione preliminare riguardante la possibile violazione occorsa, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di *Data Breach* (*violazione*)

2 - Risk assessment e individuazione misure: nel caso si stabilisca che una possibile violazione è effettivamente avvenuta, il Responsabile Protezione Dati e, in caso di *violazioni informatiche*, l'Amministratore di sistema, devono stabilire congiuntamente:le opportune misure correttive e di protezione che possano limitare i danni che la violazione potrebbe causare, se la violazione ricade nei casi un cui è necessario notificare all'Autorità Garante per la Protezione dei dati personali se l'entità della violazione necessiti di comunicare l'accadimento agli interessati.

3 - Notifica all'Autorità Garante: se è stata verificata la necessità di effettuare la notifica della *violazione dei dati*, il Titolare del trattamento della ASL Benevento provvederà alla notifica all'Autorità Garante senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

4 - Comunicazione agli interessati: se è stata valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, in quanto è stato riscontrato un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, provvederà alla comunicazione all'Interessato senza ingiustificato ritardo

Cybersecurity in ambito clinico

La cybersecurity nel settore sanitario rappresenta oggi una sfida critica e complessa. La crescente digitalizzazione dei processi clinici, la diffusione di dispositivi medici connessi in rete (IoMT - Internet of Medical Things) e la crescente interconnessione tra sistemi informativi ospedalieri espongono il settore a rischi di attacchi informatici potenzialmente devastanti, che possono compromettere la sicurezza dei pazienti, la privacy dei dati e la continuità assistenziale.

L'ambiente clinico presenta peculiarità che lo rendono un bersaglio unico:

- **Dati altamente sensibili e personali**
- **Impatto diretto sulla vita del paziente**
- **Sistemi legacy e infrastrutture eterogenee**
- **Vincoli operativi rigidi (24/7, emergenze)**
- **Necessità di disponibilità e integrità costanti**

Fonte ACN

Principali Minacce principali in ambito clinico

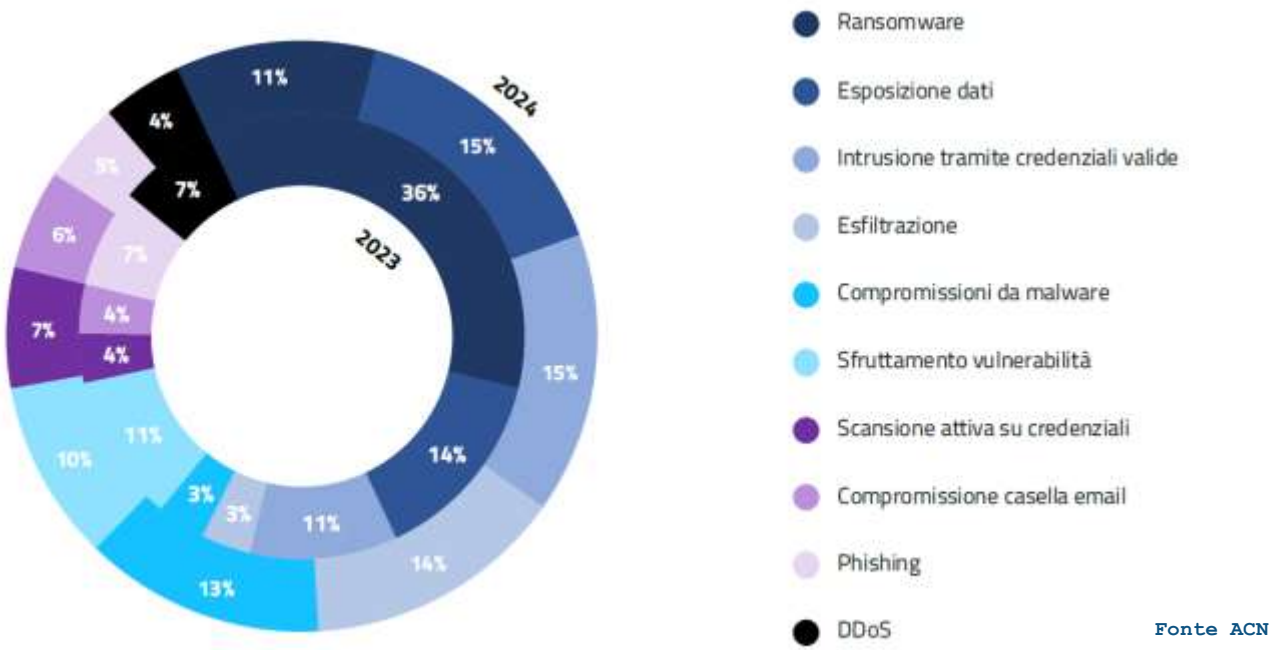
Malware e Ransomware

Phishing e Social Engineering

Accesso non autorizzato

Attacchi DDoS (Distributed Denial of Service)

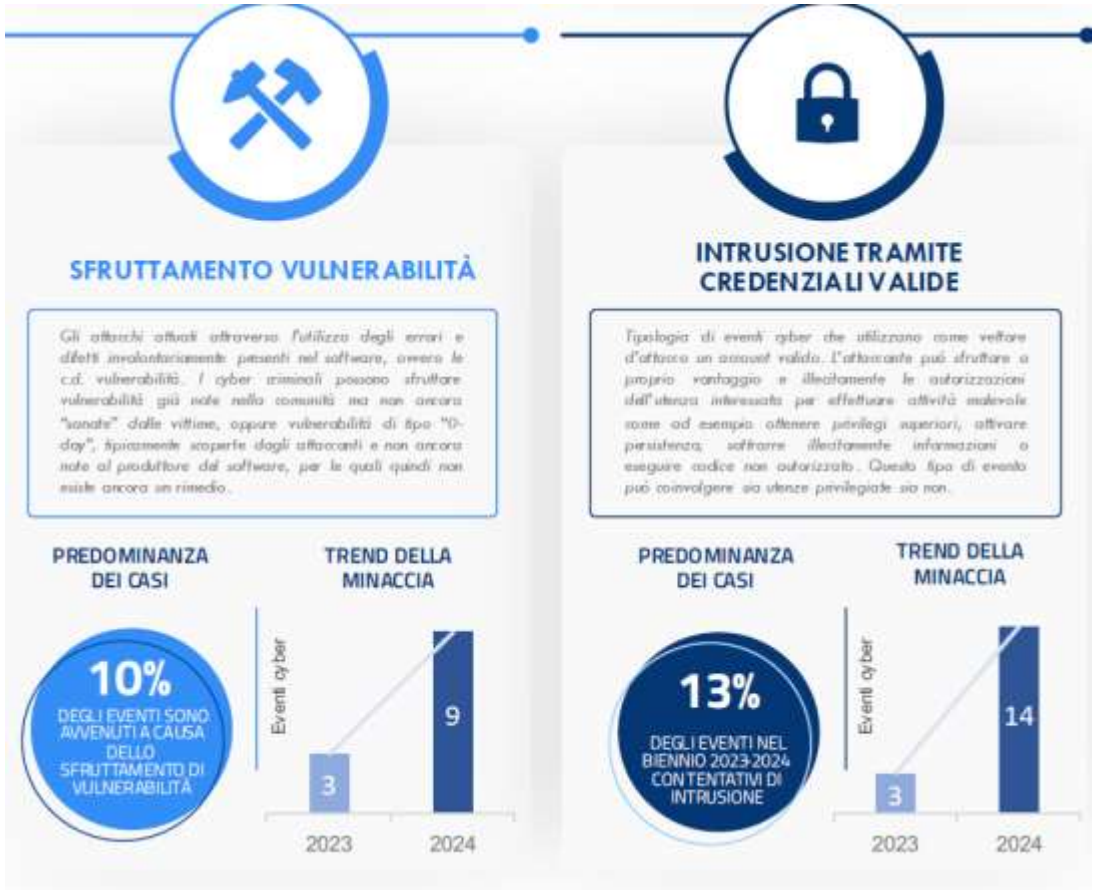
Vulnerabilità nei dispositivi medici connessi



Fonte ACN

Figura 3: tipologie di minacce rilevate negli eventi cyber nel periodo 2023-2024 (top 10)

Cybersecurity – le principali minacce



Main Security Framework

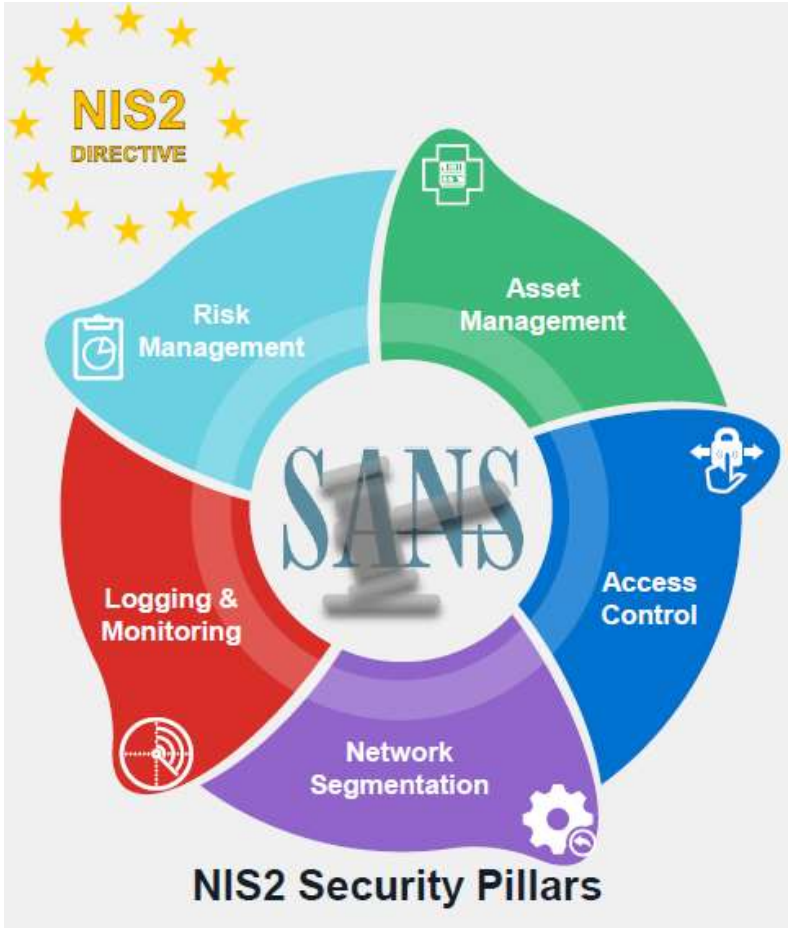
Key Frameworks	Type	Body	Origin	Scope	GEO
NIS Directives	Policies	ENISA	EU (+ UKI)	OES & DSP (*) IT/OT	EU
ISA/IEC 62443 (formerly **ISA-99**)	Standards	ISA,IEC, ANSI	International	Multi-Industry OT	Multi
IEC/ISO 27000s	Standards	ISO, IEC	International	Multi-Industry IT/OT	Multi
NERC-CIP	Standards	NERC	US	Electricity IT/OT	NAM
NIST CSF	Guidelines (Framework)	NIST	US	Multi-Industry IT/OT	Multi
NIST SP 800-82	Guidelines	NIST	US	Multi-Industry OT	Multi
NIST SP 800-53	Guidelines	NIST	US	Multi-Industry IT/OT	Multi
Critical Security Controls (CIS Top 18)	Guidelines	CIS	US	Multi-Industry OT	Multi

Direttiva NIS : i soggetti coinvolti

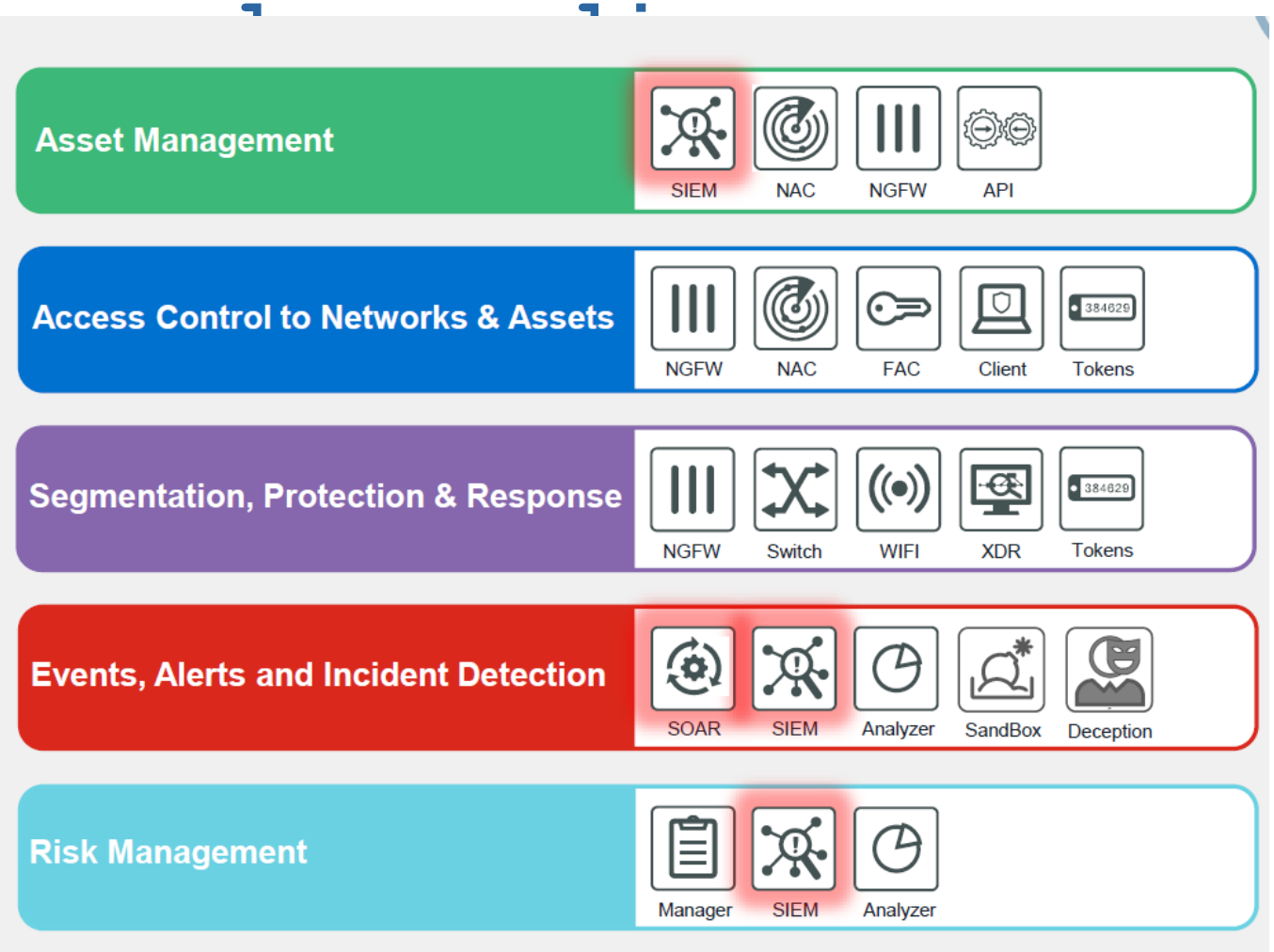
Operatori di servizi essenziali (OSE) ed Operatori di Servizi Importanti

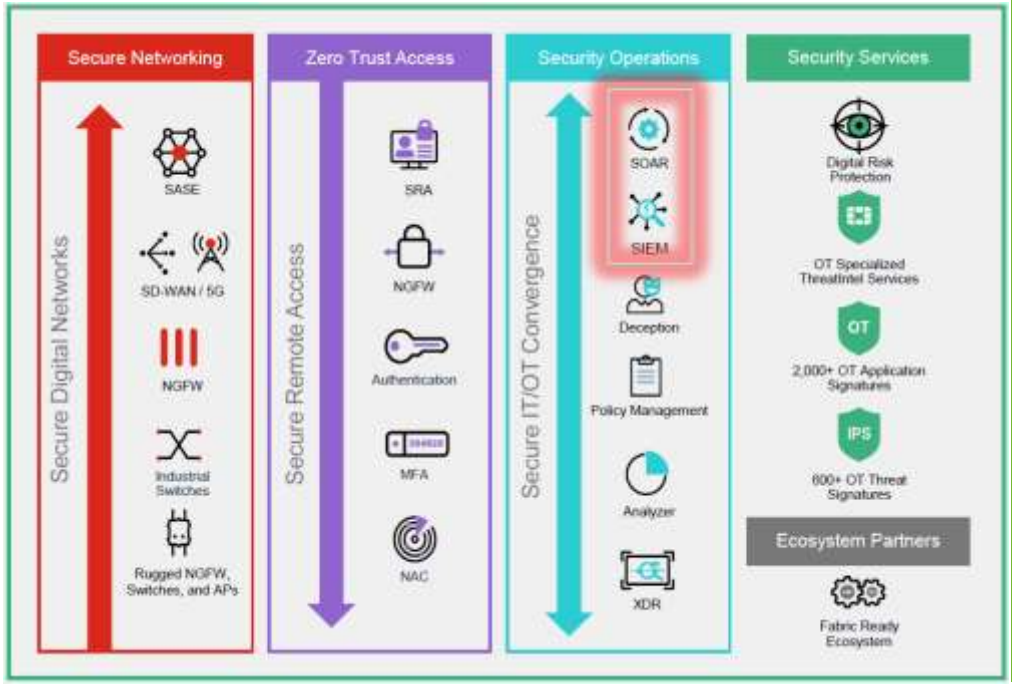
Direttiva NIS 2 : gli obiettivi

- **Politiche di analisi dei rischi** e di sicurezza dei sistemi informatici
- **Gestione** degli **incidenti**
- **Continuità operativa**, il ripristino in caso di disastro, e gestione delle crisi
- Sicurezza della **catena di approvvigionamento**
- **Sicurezza dell'acquisizione, dello sviluppo e della manutenzione** dei sistemi informatici e di rete
- Strategie e procedure per valutare l'efficacia delle **misure di gestione dei rischi**
- **Pratiche di igiene informatica** di base e formazione di cybersicurezza
- Politiche e procedure relative all'uso della **crittografia** e della **cifratura**
- **Sicurezza delle risorse umane, strategie di controllo dell'accesso** e gestione degli attivi
- Uso di **soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti** da parte del soggetto



Direttiva NIS 2 : soluzioni tecnologiche

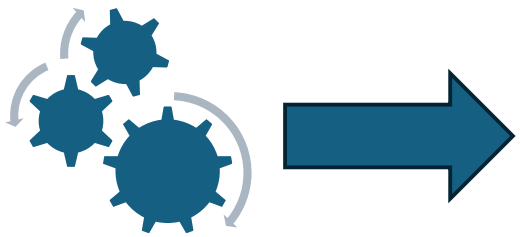




Best practice organizzative

Formazione del personale	•Corsi periodici su sicurezza informatica e riconoscimento di phishing/social engineering •Policy chiare e procedure di segnalazione di incidenti
Gestione delle identità e degli accessi	•Principle of least privilege: assegnare ai dipendenti solo i permessi necessari •Controllo degli accessi basato su ruoli (RBAC)
Monitoraggio e auditing	•Log di accesso e attività dettagliati e centralizzati •Analisi comportamentale per individuare anomalie
Valutazione delle vulnerabilità	•Penetration test regolari •Aggiornamenti tempestivi di software e firmware

Integrazione Dispositivi Medici e infrastruttura IT
Aspetti da attenzionare



Safety (E.M.)

Regolamento UE 2017/745 – DM
Art.71 D.Lgs. 81/08
Norma UNI 14971:12
Norma CEI EN 62353

Security (ICT)

Regolamento UE 2016/679 – GDPR
Norma CEI 62-237
Norma ISO 27001:13

Sicurezza DM-IT

Norma UNI ISO 80001-1

L'ambito normativo – IEC 80001-1:2021

Applicazione della gestione del rischio per reti IT che incorporano dispositivi medicali
Parte 1: Ruoli, responsabilità e attività

1 - La presente Norma definisce le funzioni, le responsabilità e le attività necessarie alla gestione dei rischi delle reti IT che incorporano dispositivi medicali ai fini della sicurezza, dell'efficienza e della sicurezza dei dati e del sistema.

2 - La Norma non specifica i livelli di rischio accettabili.

3 - La presente Norma si applica quando un dispositivo medicale è stato acquisito da un'organizzazione responsabile ed è previsto di incorporarlo in una rete IT.

4 - La presente Norma si applica a tutto il ciclo di vita della rete che incorpora DM

Criticità principali secondo la IEC 80001-1

La norma **IEC 80001-1:2021** (e la versione aggiornata **DIN EN IEC 80001-1:2023** identifica una serie di criticità ricorrenti nella gestione del rischio per reti IT che integrano dispositivi medici:

Mancanza di ruoli e responsabilità chiari: spesso non è definito chi è responsabile della sicurezza e dell'efficacia dei dispositivi connessi alla rete

- **Assenza di un processo strutturato di gestione del rischio**: molte organizzazioni non adottano un approccio sistematico per valutare e mitigare i rischi legati all'interconnessione di dispositivi medici.
- **Inadeguata documentazione delle attività**: la norma richiede tracciabilità e documentazione delle decisioni, spesso trascurate nella pratica.
- **Difficoltà nell'integrazione di software e dispositivi eterogenei**: la coesistenza di tecnologie legacy e moderne crea problemi di compatibilità e interoperabilità

Key Property secondo la IEC 80001-1

Safety

Immunità da rischi inaccettabili per il paziente, dai danni fisici al paziente (ma anche agli operatori ed a terzi) o dai danni alla proprietà o all'ambiente

i rischi possono essere provocati da:

- malfunzionamenti del DM derivanti
  - da "guasti" o "errate configurazioni" degli interfacciamenti
  - da interazioni non desiderate tra il DM e il "mondo informatico esterno"
- rischi legati alla sicurezza elettrica

effectiveness

Capacità di produrre il risultato atteso per il paziente e l'organizzazione responsabile

L' obiettivo è perseguibile principalmente tramite l'adozione di best practice internazionali e l'impiego degli standard (IHE, DICOM, HL7, SOA, ICD-9, Snomed, LoInc, ecc) per realizzare il flusso dati a partire dal DM in rete/dal software DM, al fine dell'interfacciamento, dell'integrazione e dell'interoperabilità con l'infrastruttura IT.

data and system security

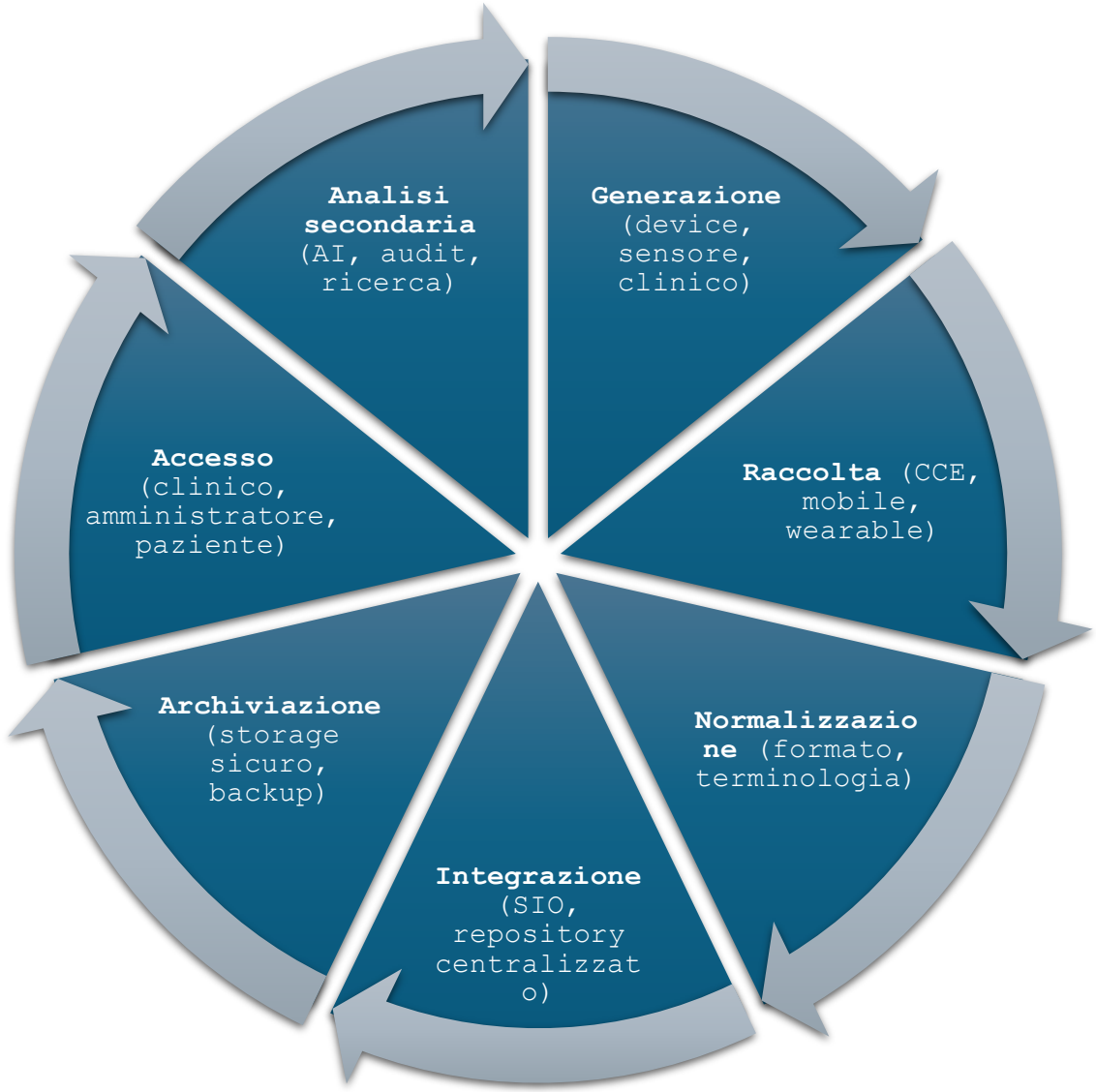
Garantire la sicurezza di dati e di sistemi che insistono sulla rete dati aziendale è un obbligo di legge definito a più livelli e sotto vari punti di vista (crimini informatici e CP, CAD e quadro normativo di riferimento, privacy e quadro normativo di riferimento) e va perseguito con una logica di sistema e non con interventi a spot.

Flusso e Gestione dei Dati Clinici

Classificazione dei Dati Sanitari

Tipo di dato	Esempi	Formato	Fonte principale
Dati strutturati	Parametri vitali, esami di laboratorio, codici ICD-10	Tabellare	LIS, CCE
Dati non strutturati	Referti testuali, note cliniche, immagini radiologiche	Testo libero, DICOM	RIS, PACS
Dati in tempo reale	ECG, monitor multiparametrico, infusori	Streaming	Dispositivi IoMT
Dati longitudinali	Storico paziente, episodi clinici	Multi-episodio	Repository clinico

Ciclo di Vita del Dato Clinico



Fonti e Destinatari dei Dati

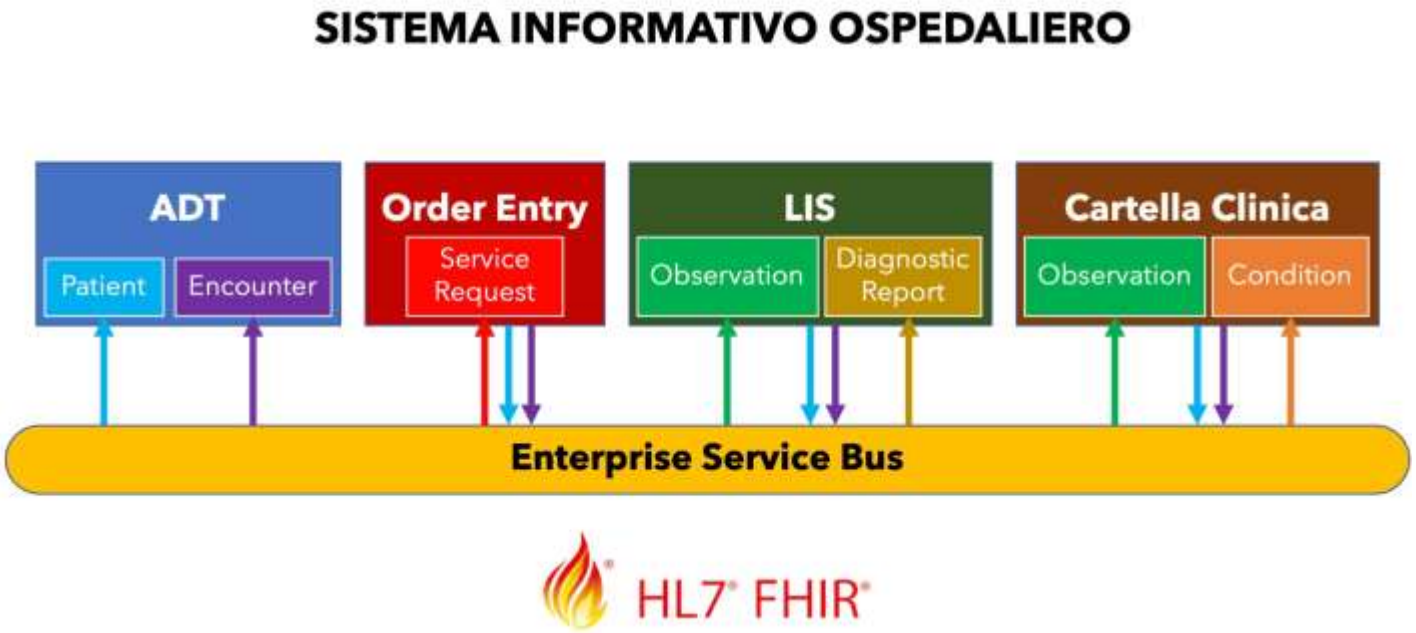
Fonte	Destinatario	Esempio di interazione
Monitor intraoperatorio	CCE	Streaming parametri
Robot chirurgico	PACS, CCE	Videoregistrazione
LIS	Medico prescrittore	Referto esame ematico

Sistemi Informativi Ospedalieri (SIO): una rete di moduli interoperabili

Il **Sistema Informativo Ospedaliero (SIO)** è l'insieme dei software che gestiscono le attività cliniche, amministrative, logistiche e di governance di un presidio sanitario. È composto da numerosi **moduli verticali**, che vanno integrati secondo standard comuni.

Moduli principali del SIO:

Questi sistemi devono comunicare tra loro e con la CCE per evitare **isole informative**, ridurre il rischio di errori clinici e garantire



Modulo	Funzione
ADT	Gestione ricoveri, trasferimenti, dimissioni
LIS	Refertazione e tracciamento esami di laboratorio
RIS/PACS	Gestione e archiviazione immagini diagnostiche
Pharmacy Information System	Prescrizione, somministrazione e tracciabilità farmaci
Sistemi di blocco operatorio	Documentazione, programmazione e reporting chirurgico
ICU/HDU Systems	Monitoraggio avanzato in terapia intensiva e subintensiva

Middleware e Architetture di Integrazione

Enterprise Service Bus (ESB)

- Centralizza il routing, la trasformazione e l'orchestrazione dei messaggi
- Supporta protocolli come HL7 v2/v3, DICOM, SOAP, REST
- Include motori di regole per la gestione dei flussi

FHIR Gateway

- Pubblicazione sicura dei dati clinici via API RESTful
- Formato JSON/XML
- Interoperabilità con applicazioni mobile, dispositivi di monitoraggio remoto e sistemi esterni

Data Integration Engine (DIE)

- Motore ETL per caricamento, trasformazione e normalizzazione dei dati
- Provenienza da diverse fonti (legacy e moderne)

Clinical Data Repository (CDR)

La Cartella Clinica Elettronica (CCE)

Cuore digitale dell'informazione sanitaria

Registrazione e conservazione dei dati

Accesso in tempo reale

Accessibilità multiutente e distribuita

Geograficamente distribuita

Supporto per dati strutturati e non strutturati

Integrazione di dati completi

Dati anagrafici e identificativi

Anamnesi e diario clinico

Referti di laboratorio e imaging

Atti e procedure terapeutiche e chirurgiche

Informazioni da dispositivi medici

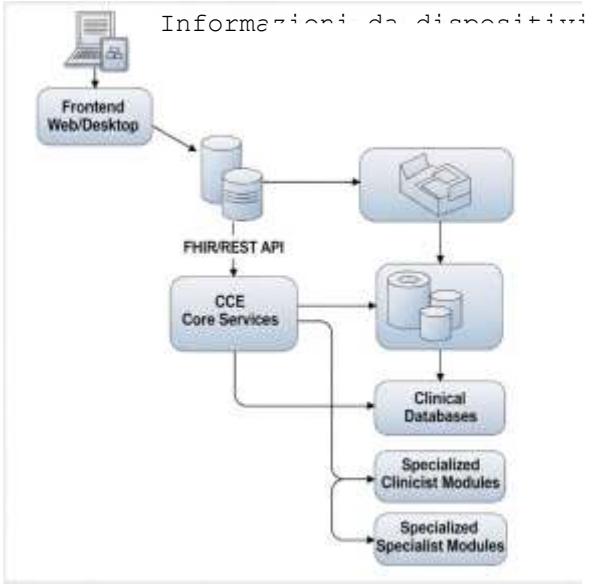
schema a blocchi della struttura CCE

Frontend Web/Desktop: Questo rappresenta l'interfaccia utente attraverso la quale gli operatori sanitari (e potenzialmente i pazienti) interagiscono con il sistema. Può essere un'applicazione web accessibile tramite browser o un'applicazione desktop dedicata. È il punto di accesso per l'inserimento, la visualizzazione e la gestione dei dati clinici.

API FHIR/REST: Si tratta di un'interfaccia di programmazione delle applicazioni (API) che funge da ponte tra il frontend e i servizi core del CCE. Utilizza standard FHIR (Fast Healthcare Interoperability Resources) per lo scambio di dati sanitari in modo standardizzato e sicuro, oltre a principi REST (Representational State Transfer) per la comunicazione tra i sistemi. Questo garantisce l'interoperabilità e la flessibilità.

CCE Core Services: Questo blocco rappresenta il cuore logico del sistema. Contiene i servizi e i processi fondamentali che gestiscono la logica aziendale, l'elaborazione dei dati clinici, la gestione degli utenti, la sicurezza e l'orchestrazione delle varie funzionalità. È qui che avvengono le operazioni chiave richieste dal frontend e gestite verso il database.

Database Clinici e Moduli Specialistici: Questo componente finale include i database veri e propri dove vengono archiviati tutti i dati clinici dei pazienti (anamnesi, diagnosi, terapie, esami, ecc.). Inoltre, comprende i "moduli specialistici",



Integrazione in Sala Operatoria Ibrida

Visionare imaging preoperatorio	Accedere al diario anestesiologico	Documentare l'intervento	Sincronizzare le informazioni
• Accesso diretto da PACS alla CCE	• Disponibile in tempo reale	• Utilizzo di interfacce touch	• Con il registro operatorio nazionale

Interoperabilità tra dispositivi multi-brand – criticità

1. Protocolli proprietari

Molti dispositivi utilizzano protocolli chiusi, senza documentazione pubblica, limitando o impedendo l'integrazione automatica.

2. Mancanza di standard condivisi

Anche quando i protocolli sono standardizzati, le implementazioni possono differire (es. HL7 v2 customizzati), causando incompatibilità operative.

3. Assenza di API aperte

Sistemi legacy o economici spesso non espongono API o SDK per accedere ai dati in modo programmabile.

4. Conflitti semantici

Lo stesso parametro può essere codificato in modo diverso da vendor differenti. Esempio: "SpO2" può essere registrato come "SPO2", "O2Sat", o "OxygenSaturation".

5. Performance e sincronia

Il flusso di dati real-time può richiedere QoS elevati (latenza <100ms), difficili da garantire in architetture generiche.

Tipologie di Interoperabilità

Livello	Descrizione
Tecnico	Compatibilità delle interfacce fisiche e protocolli di comunicazione (es. Ethernet, Wi-Fi, USB, RS-232)
Sintattico	Formato e struttura dei messaggi (es. HL7 v2, FHIR, XML, JSON)
Semantico	Comprensione uniforme dei contenuti (es. terminologie SNOMED CT, LOINC)
Organizzativo	Armonizzazione dei flussi operativi tra reparti, vendor, sistemi
Legale/Normativo	Conformità a regolamenti e norme di sicurezza

Principali Architetture di interoperabilità

1. Soluzioni point-to-point

Ogni dispositivo comunica direttamente con ogni altro sistema attraverso interfacce dedicate. È una soluzione fragile e poco scalabile.

2. Architettura a hub (middleware)

Un **integration engine** centralizza lo scambio di dati tra i dispositivi e i sistemi clinici.

3. Medical Device Integration (MDI) Platform

Piattaforme specifiche per la **medical device integration**, come Capsule Tech, iBus, o Capsule Vitals Plus,

4. Integrazione tramite gateway FHIR

Alcuni dispositivi moderni forniscono direttamente API FHIR, facilitando l'integrazione con i sistemi clinici web-based o mobile.

Gli standard di integrazione

Le esigenze applicative del mondo ICT:

- Integrazione delle diverse applicazioni
- Integrazione delle diverse tecnologie e piattaforme
- Condivisione delle informazioni

La risposta alle richieste dell'ICT è data da:

- Standard Aperti
- Architetture Aperte
- Interoperabilità

Vantaggi di standard e norme

- **Riduzione dei costi:** razionalizzazione delle attività e dei processi produttivi
- **Sviluppo di un economia** del settore di riferimento

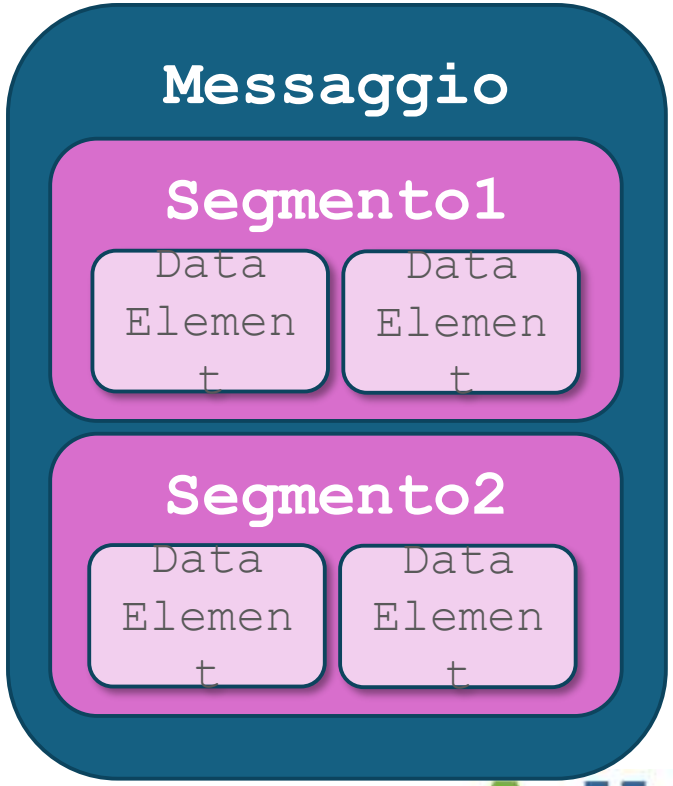
Gli standard di integrazione – HL7

Lo standard HL7 - Health Level Seven

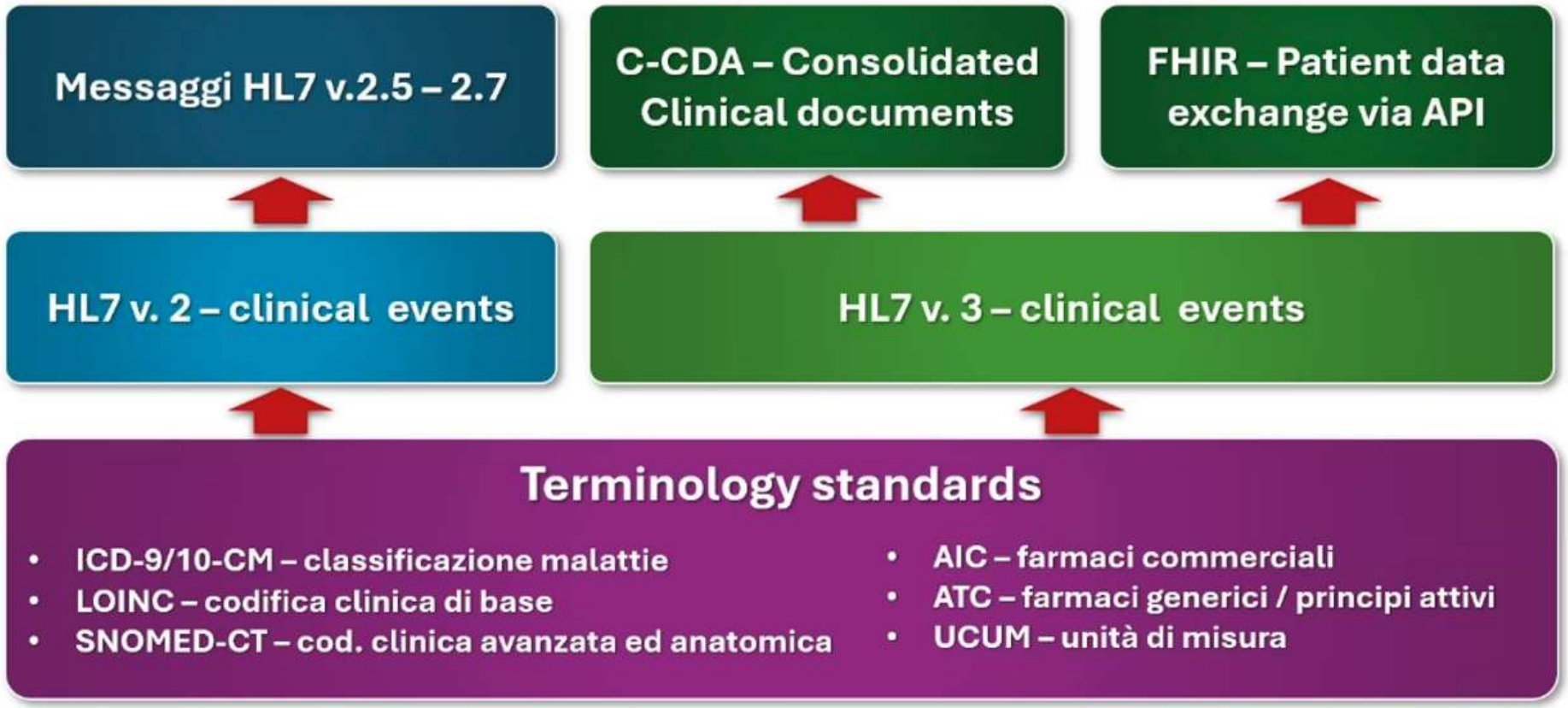
- Descrive le modalità per lo scambio in forma elettronica di dati in ambiente sanitario
- Intende risolvere i problemi legati all'interoperabilità nell'ambiente clinico

Come funzione HL7

- ✓ **Scambio concordato** di messaggi a valle di eventi prestabiliti
- ✓ **Descrive il "layout"** dei Messaggi scambiati
- ✓ Divide i Messaggi in **segmenti** e li identifica con il **nome del paziente**
- ✓ Un **Messaggio** è costituito da una sequenza ordinata di **Segmenti**
- ✓ Un Segmento è una collezione ordinata di **Data Elements**
- ✓ Tipicamente i Data Elements all'interno di un Segmento riguardano un argomento comune
- ✓ Il Tipo del Messaggio è identificato da un codice di tre lettere, e l'Evento che scatena l'inizio di una comunicazione è denominato evento **"trigger"**



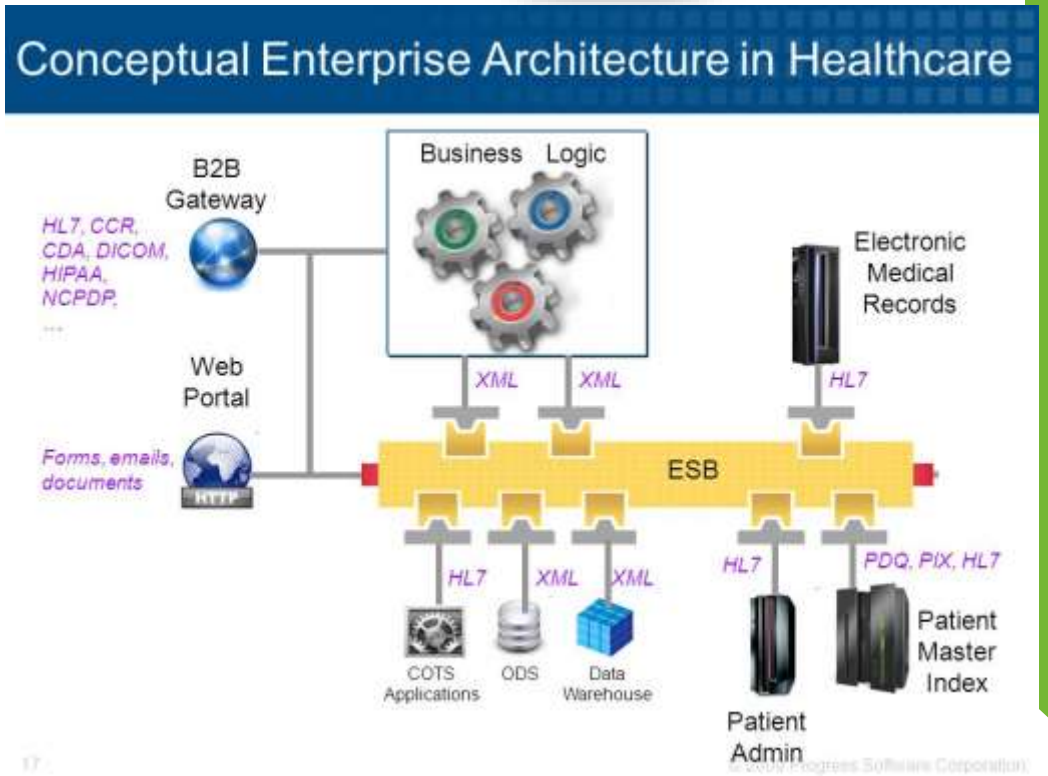
La gerarchia deli standard di integrazione HL7



Gli standard di integrazione – HL7 versione 3

HL7 Versione 3

- ✓ Modello formale di riferimento chiamato **RIM (Reference Information Model)**, basato su un unico linguaggio UML (Unified Modeling Language);
- ✓ Utilizzo **XML** per la sintassi dei messaggi;
- ✓ Standard per i documenti clinici **CDA (Clinical Document Architecture)**
  - ➢ **Clinical Document Architecture (CDA)** rappresenta un modello di scambio di documenti in ambito clinico con vari livelli di Complessità
  - ➢ Il CDA è un documento **scritto in XML** che può contenere testi, immagini, suoni ed altri contenuti multimediali



Fonte: *Progress Data Integration in Healthc*

Clinical Data Architecture

- Lo standard CDA definisce la struttura e la semantica di DOCUMENTI CLINICI con lo scopo di scambiare record di informazioni (e.g., una lettera di dimissione, un referto di laboratorio)
- L'informazione è comunque scambiata tramite messaggi ma il contenuto è un oggetto intero che include testi, immagini, dati, etc
- Il documento CDA esiste indipendentemente dal messaggio che lo trasporta

CDA è stato sviluppato come parte del progetto HL7 v3 e ne condivide la base concettuale, ovvero il **Reference Information Model (RIM)**

Il **RIM** (Reference Information Model) è un modello di riferimento fondamentale per la standardizzazione delle informazioni cliniche.

Componenti del RIM

Entità: Le entità sono gli elementi fondamentali del RIM e rappresentano oggetti o concetti nel dominio sanitario, come pazienti, diagnosi, trattamenti e osservazioni.

Attributi: Gli attributi sono le caratteristiche delle entità che descrivono proprietà specifiche, come il nome del paziente, il codice della diagnosi o la dose di un farmaco.

Relazioni: Le relazioni definiscono come le entità sono collegate tra loro.

Struttura di Base di un Documento CDA2

Un documento CDA2 è costituito da due parti principali: l'intestazione (Header) e il corpo (Body). Entrambe sono essenziali per l'organizzazione e la comprensione delle informazioni cliniche.

Intestazione (Header)

L'intestazione di un documento CDA2 contiene i metadati che descrivono il documento stesso. Questi metadati includono informazioni cruciali come:

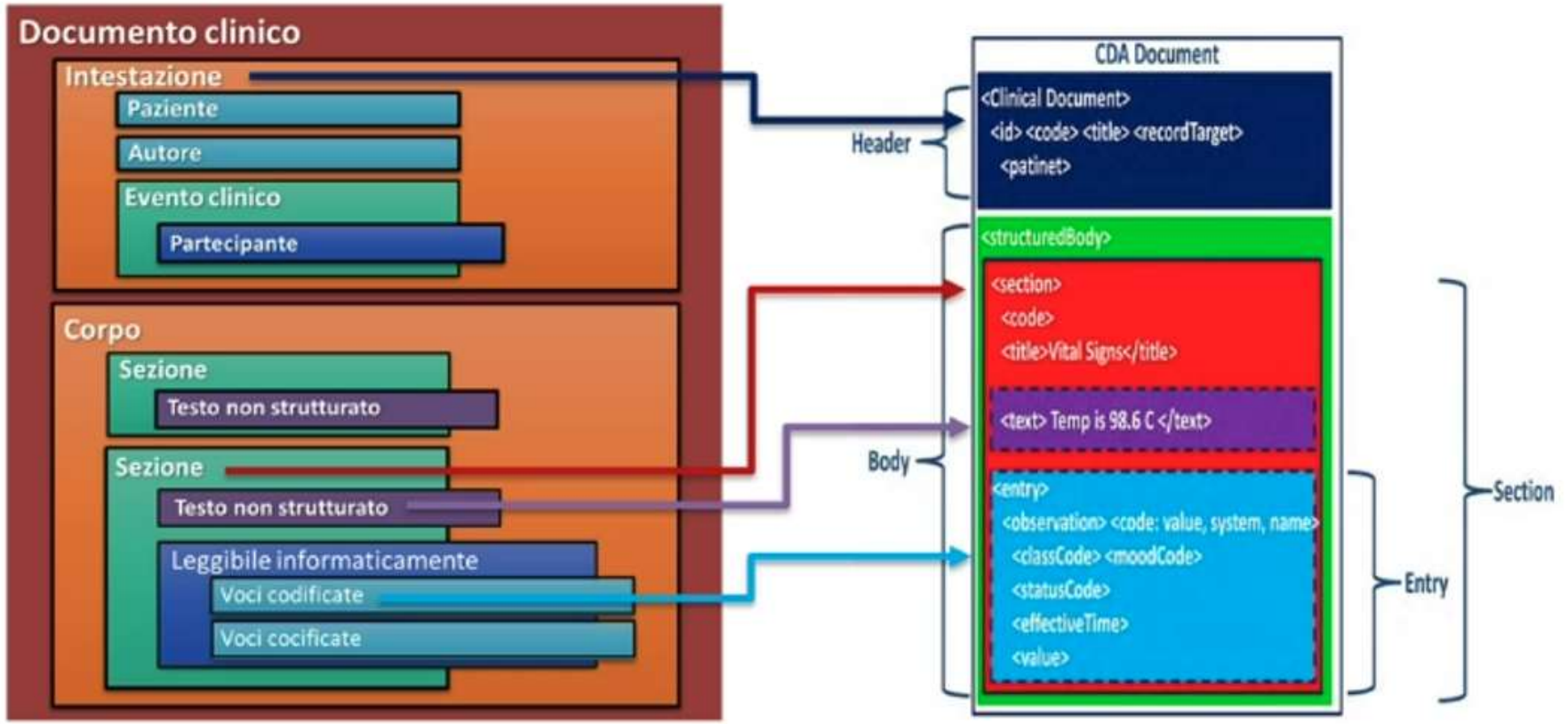
- Identificativo del documento: Univoco per ogni documento, assicura che ogni documento possa essere individuato e referenziato senza ambiguità.
- Tipo di documento: Specifica la natura del documento, come una lettera di dimissione, un referto di laboratorio o una nota di progressione.
- Data e ora di creazione: Indica quando il documento è stato creato, garantendo la tracciabilità temporale delle informazioni cliniche.
- Informazioni sul paziente: Include dettagli come il nome, la data di nascita e l'identificativo del paziente, assicurando che il documento sia correttamente associato alla persona giusta.
- Autore e firmatario: Nomi e ruoli dei professionisti sanitari che hanno creato e approvato il documento, garantendo trasparenza e responsabilità.

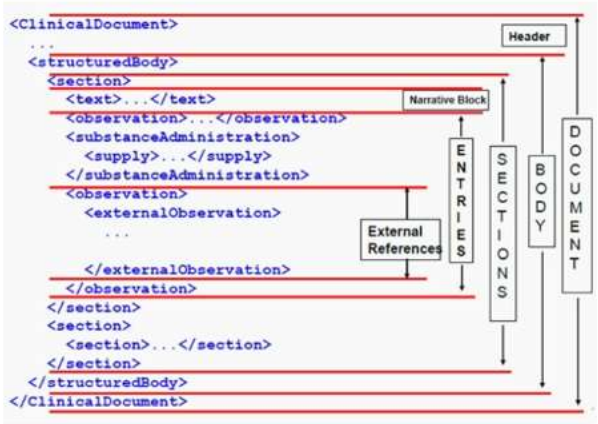
Corpo (Body)

Il corpo del documento CDA2 contiene il contenuto clinico vero e proprio. È strutturato in sezioni che possono variare a seconda del tipo di documento. Alcune delle sezioni più comuni includono:

- Storia clinica: Dettagli sui precedenti medici del paziente, comprese le condizioni croniche, le allergie e i trattamenti passati.
- Esame fisico: Risultati degli esami fisici condotti durante la visita medica.
- Diagnosi: Diagnosi attuali del paziente, basate sui sintomi e sui risultati degli esami.
- Piani di trattamento: Raccomandazioni e piani d'azione per il trattamento del paziente, compresi farmaci prescritti e terapie consigliate.
- Note di progressione: Aggiornamenti sullo stato del paziente durante il trattamento, registrati in visite successive.

Struttura di Base di un Documento CDA2





Il Profilo IHE per integrazione documenti: XDS.b

IHE (Integrating the Healthcare Enterprise) è un'iniziativa volta a migliorare l'interoperabilità dei sistemi informatici sanitari.

Uno dei profili più importanti sviluppati da IHE è il profilo **XDS.b (Cross-Enterprise Document Sharing)**, che fornisce uno standard per la condivisione e l'accesso ai documenti clinici tra diverse entità sanitarie.

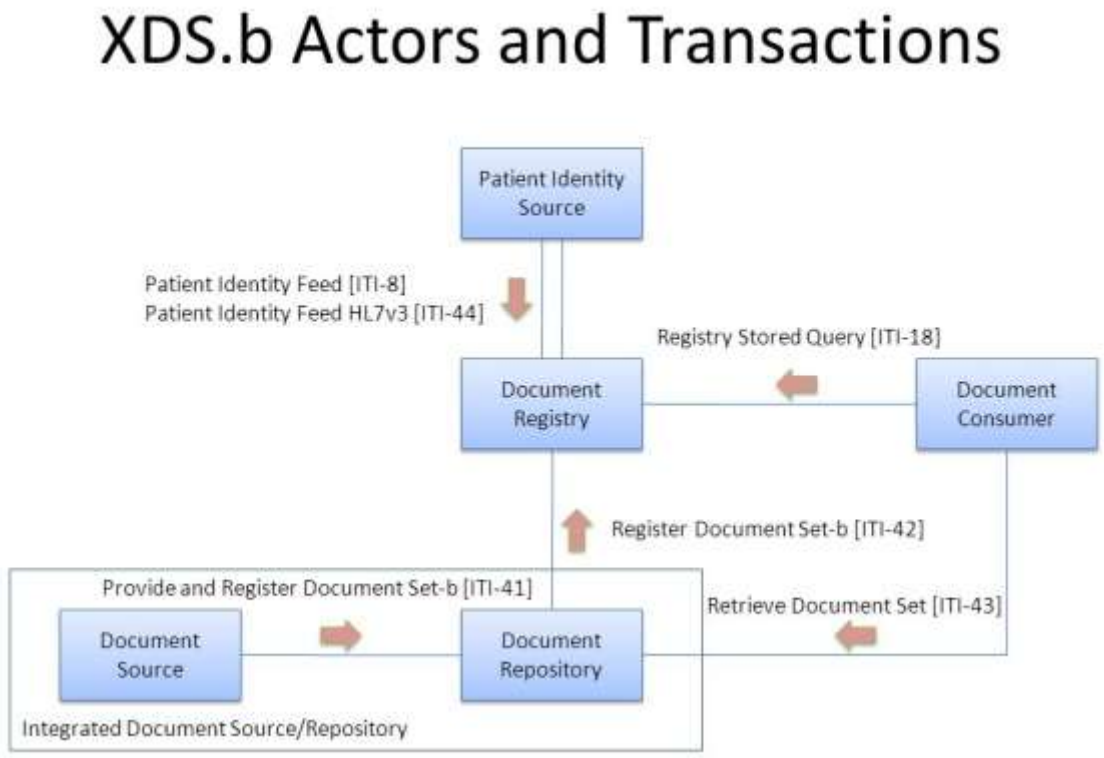
Che cos'è IHE XDS.b?

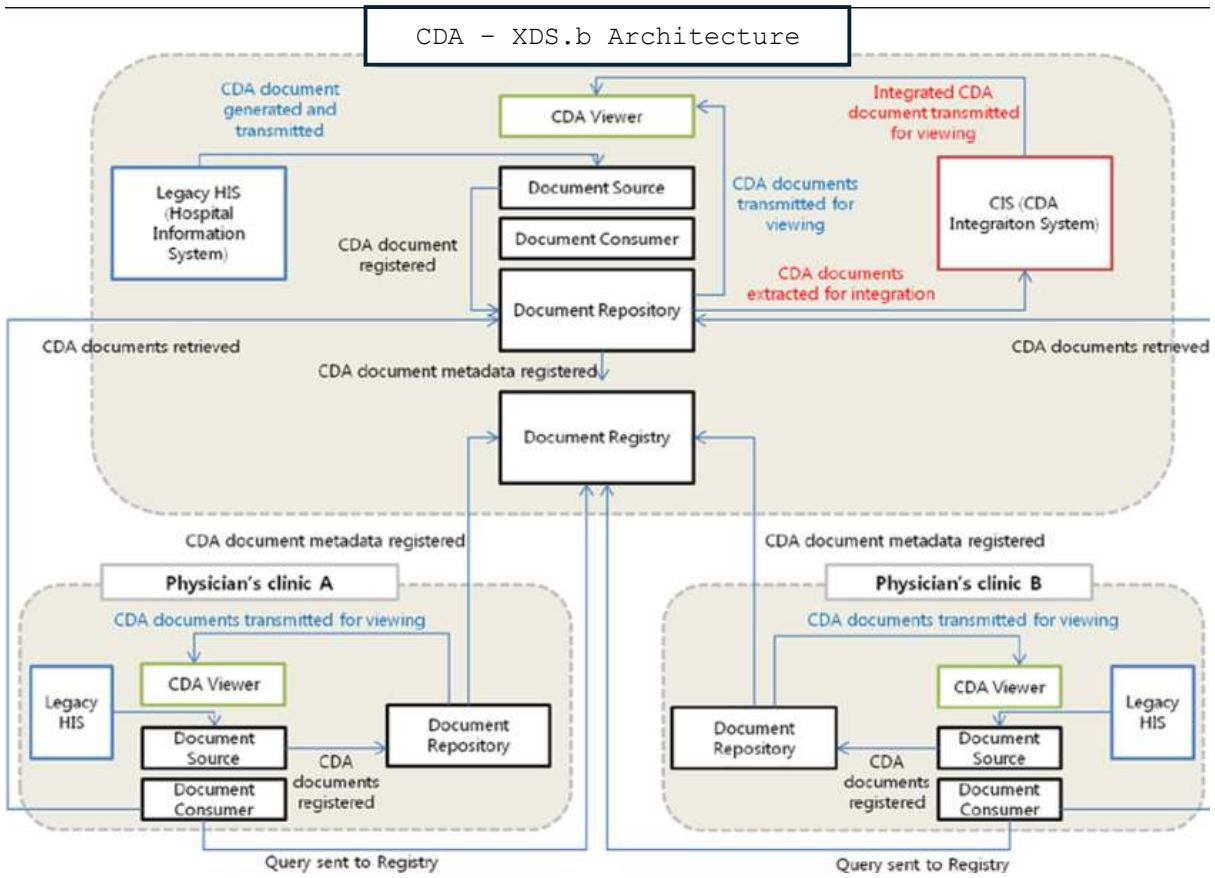
IHE XDS.b è un profilo di integrazione che definisce un sistema per la registrazione, la condivisione e il recupero di documenti clinici elettronici.
L'obiettivo principale è facilitare l'accesso ai dati clinici dei pazienti in modo sicuro e standardizzato, indipendentemente dal luogo in cui sono stati originariamente creati.

Componenti principali di IHE XDS.b

Repository Documenti: Questo componente è responsabile dell'archiviazione fisica dei documenti clinici. I documenti vengono memorizzati in un formato standardizzato, che consente un facile accesso e recupero.
Registro Documenti: Il registro documenti è un database centrale che contiene metadati sui documenti memorizzati nei repository. Questi metadati includono informazioni come l'identificatore del documento, il paziente associato, il tipo di documento e la data di creazione.
Attore Fornitore: Gli attori fornitori sono i sistemi che creano e inviano documenti clinici ai repository. Possono includere sistemi di gestione delle cartelle cliniche elettroniche (EMR), sistemi di laboratorio e altri sistemi clinici.

Integrazione documentale tramite il profilo IHE





HL7 FHIR

FHIR (Fast Healthcare Interoperability Resources) è uno standard sviluppato da HL7 (Health Level Seven International) per il trasporto di dati sanitari elettronici. È progettato per facilitare l'interoperabilità fra i diversi sistemi informativi sanitari, consentendo uno scambio efficiente e sicuro delle informazioni cliniche.

Struttura di una risorsa FHIR

Una risorsa FHIR rappresenta una singola unità di informazione che può essere utilizzata, visualizzata e scambiata in vari contesti. Le risorse sono modulari, componenti atomici che possono essere combinati e riusati per costruire soluzioni più complesse. Ogni risorsa FHIR è definita da una struttura specifica che include

Metadati

I metadati contengono informazioni sul contesto della risorsa, come l'identificatore univoco, la data di creazione e le versioni. Esempi includono:

- id: Un identificatore univoco per la risorsa.
- meta: Include informazioni come versionId, lastUpdated e profile.
- language: Specifica la lingua utilizzata nella risorsa.

Elementi di Base

Ogni risorsa contiene un insieme di elementi di base che forniscono informazioni chiave. Questi includono:

- identifier: Uno o più identificatori che forniscono un riferimento unico alla risorsa.
- status: Indica lo stato corrente della risorsa, come active, inactive, o draft.
- code: Un codice standardizzato che identifica il tipo di risorsa.

Dati Clinici

Le risorse FHIR sono progettate per contenere dati clinici specifici. Per esempio, una risorsa di tipo "Patient" include:

- name: I nomi del paziente.
- gender: Il genere del paziente.
- birthDate: La data di nascita del paziente.

Relazioni

Le risorse possono essere correlate tra loro tramite riferimenti. Questo permette di creare una rete di informazioni connesse che rappresenta la complessità delle interazioni cliniche..

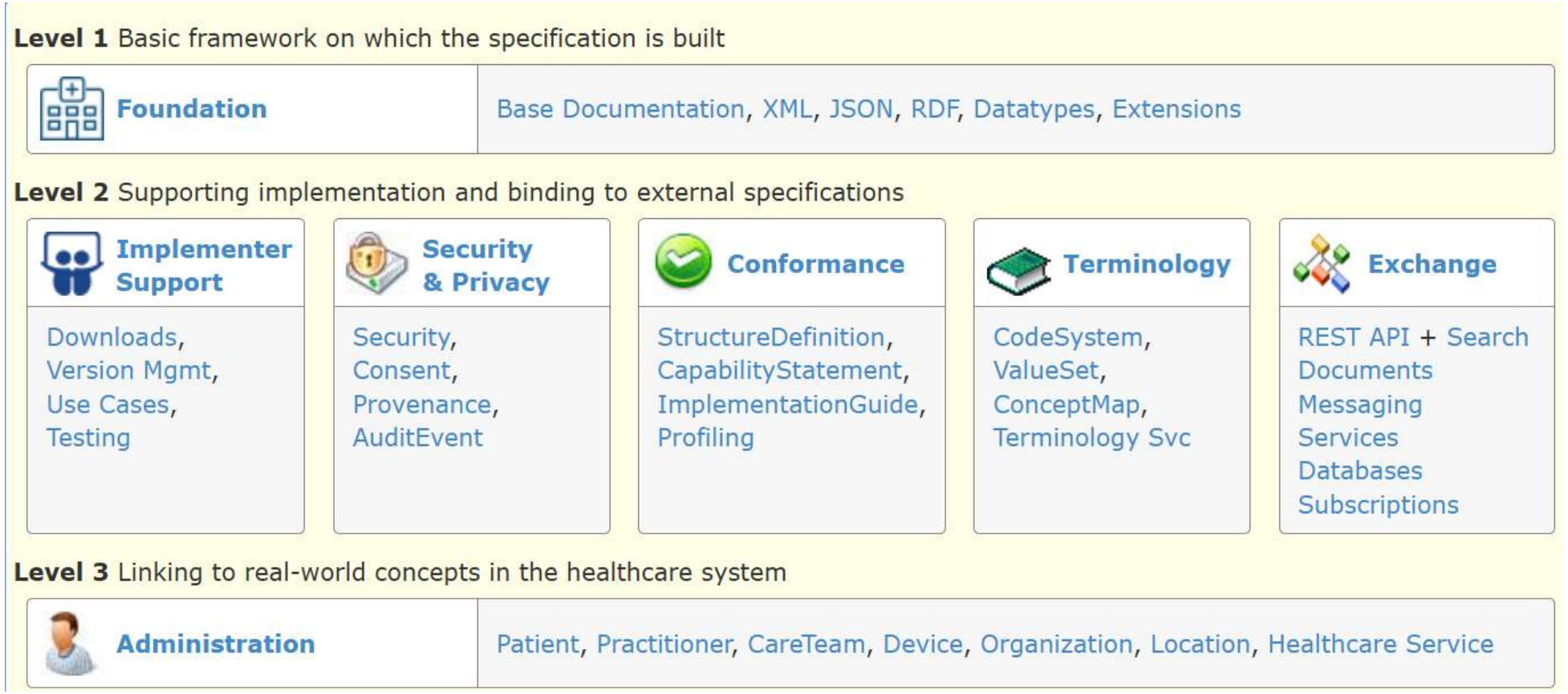
HL7 FHIR

http://build.fhir.org/modules.html

Caratteristica	**FHIR**	**HL7 v3**	**CDA**
Architettura	RESTful API	Document-centric, XML	Document-centric, XML
Modello informativo	Risorse modulari ("Resources")	RIM (molto formale e astratto)	RIM + Template
Formato dati	JSON, XML	XML	XML
Flessibilità	Elevata, facile da implementare	Bassa	Media
Adozione moderna	Crescente (soprattutto in cloud)	Limitata	Alta in documentazione clinica
Uso principale	App, interoperabilità in tempo reale	Scambio completo di contesti	Scambio di referti strutturati

HL7 FHIR

http://build.fhir.org/modules.html



HL7 FHIR

http://build.fhir.org/modules.html

Level 4 Record-keeping and Data Exchange for the healthcare process

Clinical	Diagnostics	Medications	Workflow	Financial
Allergy, Problem, Procedure, CarePlan/Goal, Family History, RiskAssessment, etc.	Observation, DiagnosticReport, Specimen, ImagingStudy, MolecularSequence, DocumentReference, ServiceRequest, etc.	Medication, Request, Dispense, Administration, Statement, Immunization, etc.	Introduction + Task, Appointment, Schedule, Referral, PlanDefinition, etc.	Claim, Account, Invoice, ChargeItem, Coverage + Eligibility Request & Response, ExplanationOfBenefit, etc.

Level 5 Providing the ability to reason about the healthcare process

Clinical Reasoning	Medication Definition
Library, PlanDefinition & GuidanceResponse, Measure/MeasureReport, etc.	Medicinal, Packaged & Administrable product definitions, Regulated Authorization, etc.

Gli standard di integrazione - DICOM

DICOM

(Digital Imaging and COmmunications in Medicine, immagini e comunicazione digitali in medicina) è uno standard che definisce i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni di tipo biomedico quali ad esempio immagini radiologiche

- ✓ **Metodo per incapsulare i dati** e per definire come questi debbano essere codificati o interpretati (non definisce alcun nuovo algoritmo di compressione)
- ✓ L'immagine viene archiviata in **forma non compressa**, secondo la codifica con la quale viene prodotta
- ✓ Esistono molti software che sono in grado di **produrre o interpretare file DICOM** contenenti dati compressi secondo vari algoritmi (JPEG, JPEG Lossless, vari algoritmi dello standard JPEG 2000, ecc.).

Gli standard di integrazione – DICOM in XML-CDA

DICOM in XML-CDA

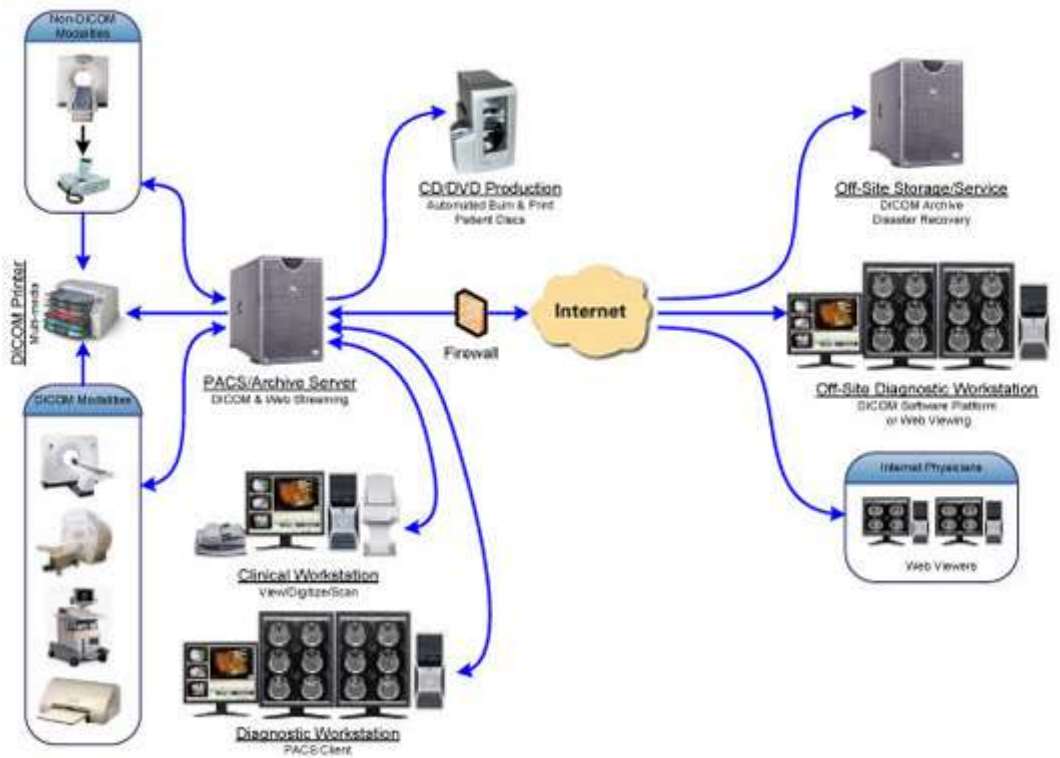
Rappresentazione degli oggetti DICOM all'interno della struttura XML-CDA

Controllo delle immagini attraverso dispositivi collegati in rete

E' necessario:

- ✓ Offrire facilità, velocità e sicurezza nell'acceso alle immagini,
- ✓ Qualità nella loro visualizzazione,
- ✓ Trasferimento efficiente verso altre stazioni di lavoro remote
- ✓ Utilizzo standard, in particolare DICOM v 3.0 e HL7 v 3.0..

Sistemi per il controllo delle immagini ➔ **PACS** (Picture Archiving and Communications Systems)



Gli standard di integrazione – XML CDA 2 - DICOM

Struttura ad albero: radice + insieme di nodi (elementi o tag).

Struttura Header

- **id** : Identificativo univoco del documento
- **code** : Codifica LOINC
- **effectiveTime** : Data di creazione del documento
- **author** : Persona che valida il documento
- **custodian** : Struttura che ha generato il referto
- **recordTarget** : Anagrafica Paziente
- **title** : Testo d'intestazione del documento
- **setId** : Identificativo comune ad ogni revisione del documento
- **versionNumber** : Versione del documento
- **legalAuthenticator** : Firmatario del referto
- **informationRecipient** : Unità di consegna
- **dataEnterer** : Rappresenta la persona che inserisce i dati nel sistema
- **responsibleParty** : Primario della struttura che ha generato l'atto
- **relatedDocument** : Collegamento tra due documenti
- **documentationOf** : Motivo della richiesta di indagine
- **inFulfillmentOf** : Order Filler
- **componentOf** : Order Placer e Unità richiedente

Conclusioni

l'oggetto del desiderio: una originale caffettiera del masochista. Deisgn: Jacques Carelmann

La tecnologia non può essere separata dall'organizzazione in cui opera né dai suoi utilizzatori, ma coevolve con essi contribuendo a nuove forme organizzative

AIIC 2025 CONVEGNO NAZIONALE ASSOCIAZIONE ITALIANA INGEGNERI CLINICI

NAPOLI 14-17 GIUGNO 2025 MOSTRA D'OLTREMARE

AIIC associazione italiana ingegneri clinici

Grazie per l'attenzione !

TECNOLOGIE, SOSTENIBILITÀ, AMBIENTE
Il contributo dell'innovazione alla sanità del futuro