Progettare per la Sanità

Organizzazione, tecnologia, architettura

04_19

CNETO
Centro Nazionale
per l'Edilizia
e la Tecnica Ospedaliera

Il progetto innovativo del **New Children's Hospital** / A colloquio con **Anton Giulio Piga** tra i massimi esperti in Talassemia / I **giardini pensili** alla base della terapia / **Telemedicina** strumento sostenibile per il SSN / Indagine sul livello di sicurezza dei **dispositivi medici connessi** / Le criticità nella distribuzione di **gas medicali**

La sicurezza nei **sistemi informativi sanitari** e nei dispositivi medici connessi

I risultati dello studio condotto dall'ALTEMS per analizzare, secondo l'approccio multidimensionale di Health Technology Assessment, il livello di sicurezza dei dispositivi medici connessi con il sistema informativo nel contesto delle aziende sanitarie italiane

Il New Children's Hospital di Helsinki
Progetto SARC Architects

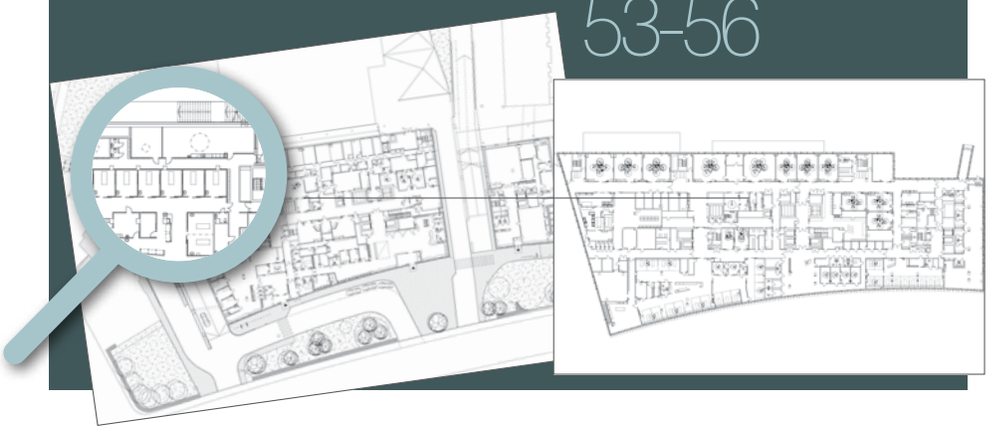
ISSN: 17206642

edra

Sommario

RUBRICHE

I PROGETTI IN **GRANDE FORMATO** DELLE ARCHITETTURE DI QUESTO NUMERO



Le aziende presenti in questo numero

di Fabrizio Massimo Ferrara

La sicurezza nei **sistemi informativi sanitari** e nei dispositivi medici connessi

I risultati dello studio condotto dall'ALTEMS per analizzare, secondo l'approccio multidimensionale di Health Technology Assessment, il livello di sicurezza dei dispositivi medici connessi con il sistema informativo nel contesto delle aziende sanitarie italiane

È ormai ampiamente riconosciuto che in un'azienda sanitaria moderna il sistema informativo non può essere un semplice insieme di tecnologie e programmi software più o meno correlati fra loro, ma deve rappresentare uno strumento completo ed integrato per il governo della struttura, sia dal punto di vista della gestione corrente che sotto il profilo della strategia evolutiva, assicurando la continuità dei processi aziendali attraverso i diversi settori e l'integrazione e la disponibilità del patrimonio informativo sotto il profilo sia clinico che amministrativo. E questo sia all'interno dell'azienda che nel contesto della rete territoriale per la continuità del percorso assistenziale del paziente.

In una tale visione, una valenza particolare assume ovviamente la gestione della "sicurezza" (includendo in questo termine anche gli aspetti di protezione dei dati personali, secondo quanto prescritto dal recente Regolamento UE 2016/679), che va intesa non solo dal punto di vista prettamente tecnologico, ma in quadro più ampio, tale da garantire l'esecuzione sicura e corretta dei processi aziendali, minimizzando e prevenendo –per quanto possibile– tutti i rischi ai quali l'azienda può essere esposta. Rischi che –nel settore sanitario– assumono una rilevanza particolare in quanto possono avere implicazioni anche sulla stessa salute del paziente.

In questa visione maggiormente strategica, anche le modalità organizzative secondo cui viene valutato, monitorato ed evoluto il sistema informativo e le caratteristiche sue funzionali ed informative costituiscono quindi elementi fondamentali e qualificanti ai fini della sicurezza e della gestione del rischio.

In estrema sintesi l'obiettivo finale di un **sistema informativo sicuro** può essere individuato nella capacità:

a. di seguire e supportare senza soluzione di continuità i processi dell'organizzazione (sia quelli che si esauriscono all'interno di un singolo settore che –soprattutto– quelli che si articolano attraverso settori diversi e sul territorio);
b. di integrare e proteggere i dati raccolti attraverso applicazioni, contesti e dispositivi anche eterogenei rendendoli disponibili quando e come necessario alle persone autorizzate;
c. di fornire un contributo attivo nell'identificazione di rischi e situazioni di allarme, anche correlando autonomamente informazioni diverse, anche nel caso di co-morbilità e dimenticanze da parte dell'utente.

Il tutto supportato da una infrastruttura tecnologica robusta ed affidabile e gestito secondo una organizzazione e criteri formalizzati e misurabili, secondo principi di monitoraggio continuo e miglioramento progressivo.

In un tale scenario, la gestione della sicurezza nei sistemi informativi e la definizione di strategie evolutive, che tengano con-

to sia delle possibilità connesse a nuovi modelli organizzativi e a nuove tecnologie sia delle normative sempre più precise e stringenti, si deve necessariamente basare su un approccio multidimensionale che tenga conto di tutte le caratteristiche e di tutti gli aspetti che incidono di fattori di rischio (fig. 1).

LA SICUREZZA NEI DISPOSITIVI MEDICI CONNESSI

Secondo questo approccio, è stato condotto uno studio per analizzare per gli aspetti di sicurezza specifici dei contesti -sempre più rilevanti- in cui i dispositivi medici elettronici rivestono un ruolo significativo nel processo assistenziale e di cura.
Va infatti considerato che sempre di più le prestazioni erogate sono basate su un impiego intensivo di apparecchiature e dispositivi medici connessi con il sistema (IDC stima che entro il 2020 il 16% dei dati sanitari sarà proveniente da dispositivi medici, inclusi gli scenari di IoT).
Il contesto del sistema informativo si amplia quindi fino ad includere dispositivi medici, e la sicurezza complessiva dipende sempre di più dalla sicurezza del binomio "sistema informativo + dispositivi connessi", come evidenziato nella figura 2.

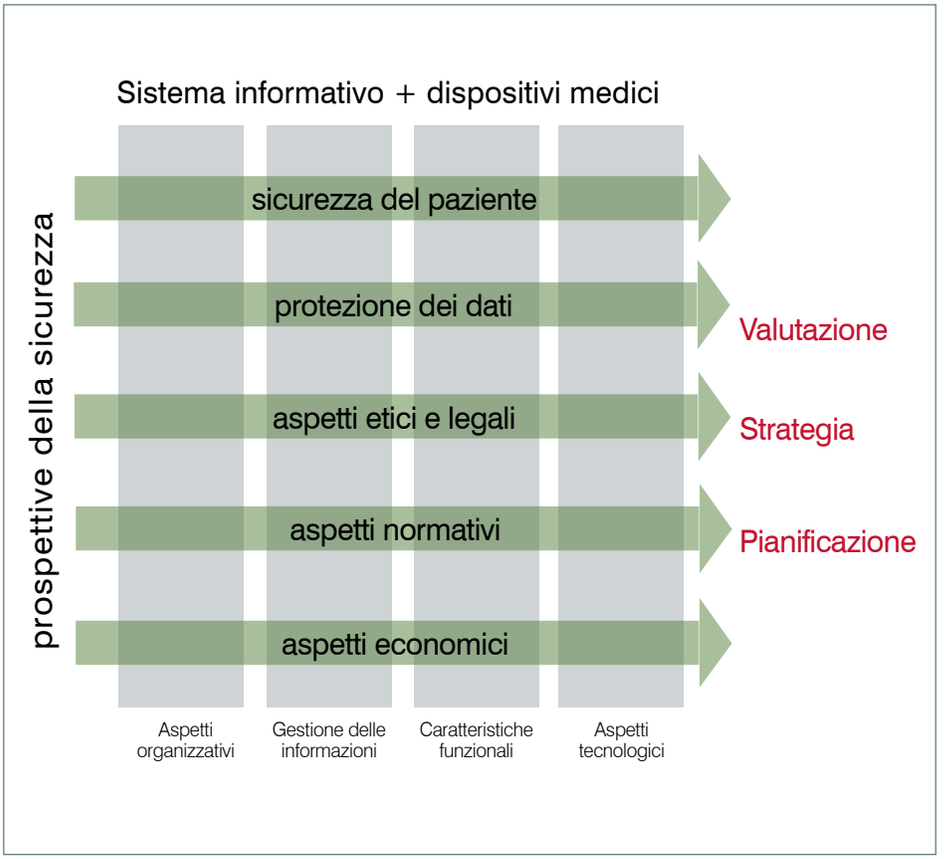


Figura :1 L'approccio multidimensionale dell'HTA per valutare e gestire la sicurezza del sistema informativo nel suo complesso

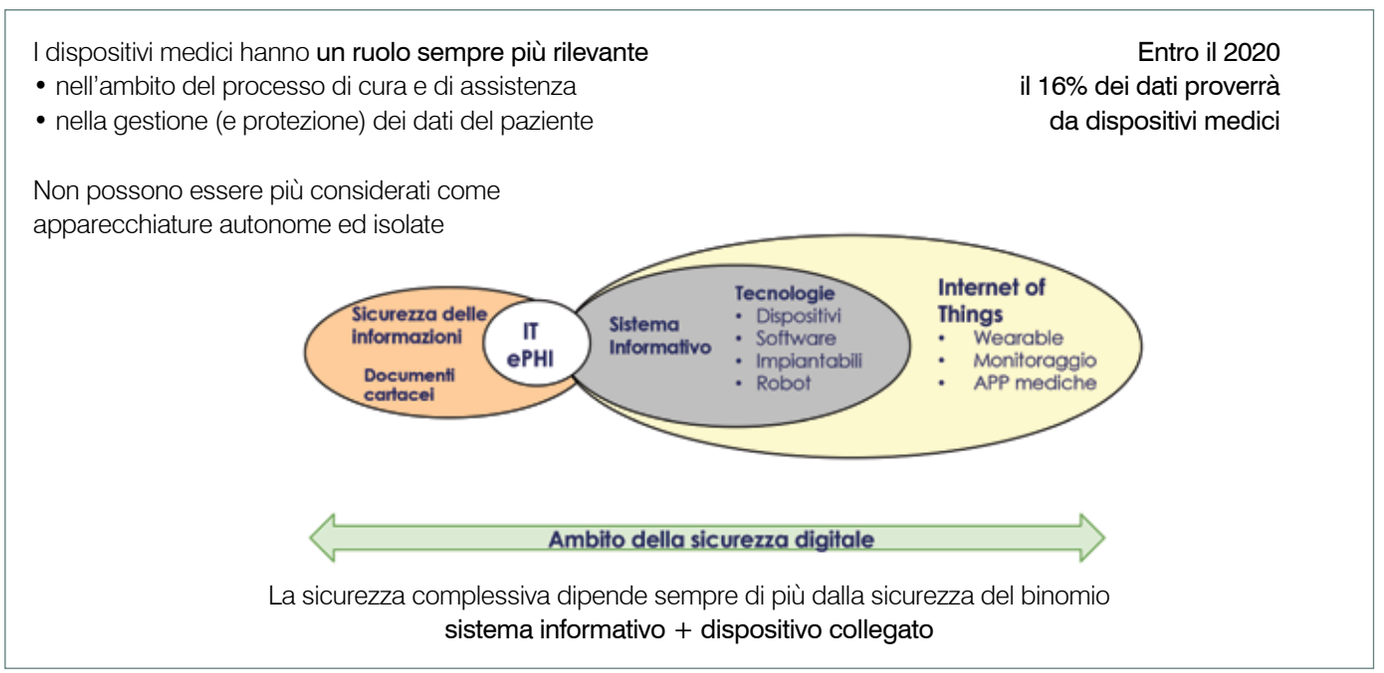


Figura 2: La rilevanza dei dispositivi medici

RISULTATI DELL'INDAGINE

L'indagine ha coinvolto 112 presidi ospedalieri dalla quasi totalità delle regioni italiane, che hanno fornito informazioni (per un totale di oltre 17.000 dati raccolti) sulle caratteristiche del loro sistema informativo e dei dispositivi medici connessi.

I dispositivi medici connessi presentano una varietà di caratteristiche e di utilizzo estremamente ampia (dal robot operatorio all'IoT). Una analisi indiscriminata di tutti i contesti non porterebbe quindi a risultati significativi. Per consentire la validità generale del modello, indipendente dalle specifiche patologie e processi clinici, i dispositivi sono stati quindi classificati in funzione del loro ruolo all'interno del processo assistenziale e delle modalità di utilizzo nel contesto organizzativo:

- dispositivi "**individuali**": quelle apparecchiature utilizzabili individualmente da parte del paziente (all'esterno o all'interno del centro) e/o da personale sanitario nell'ambito dell'attività clinica e/o assistenziale per la rilevazione di parametri (es. strumenti commerciali, ECG ed altra strumentazione portatile, misuratori portatili di valori ematici, etc.). Rientrano in questo contesto anche i dispositivi genericamente individuati nel "mondo IoT".
- dispositivi "**condivisi**": quelle apparecchiature in dotazione all'interno di una specifica UO della struttura per la misurazione di parametri vitali e/o l'effettuazione di esami diagnostici complementari alle attività cliniche della struttura stessa (es. ecografi, flussimetri, ecc.). Operano autonomamente (collegate o meno con il sistema sanitario centrale dell'organizzazione) e non necessitano di sistemi informatici articolati e complessi per il loro controllo.
- dispositivi "**centralizzati**": quelle apparecchiature di alto costo e complessità, collegate con e controllate da sistemi informatici complessi e dedicati (cosiddetta diagnostica "pesante", apparecchiature di laboratorio, robot chirurgici, ecc.) stabilmente installate all'interno di UO della struttura, e costituenti strumenti essenziali e critici per l'effettuazione delle attività della UO stessa. Oltre che per il loro numero relativamente ridotto, per motivi di costo, complessità e rilevanza clinico/organizzativa, queste apparecchiature "centralizzate" sono usualmente acquisite, installate e gestite nell'ambito di processi e procedure formalizzate, valide per tutta la struttura.

Secondo questi criteri, i principali ambiti di utilizzo dei dispositivi, all'interno dell'organizzazione ed in contesti di telemedicina, sono rappresentati in figura 4.

Gli indicatori raccolti mediante l'indagine si riferiscono alle quattro prospettive tipiche di analisi dei sistemi informativi: aspetti organizzativi, aspetti informativi, aspetti funzionali, aspetti tecnologici.

Dal punto di vista organizzativo, è innanzi tutto da osservare come - a livello complessivo- in circa il 70% dei casi non esista una col-

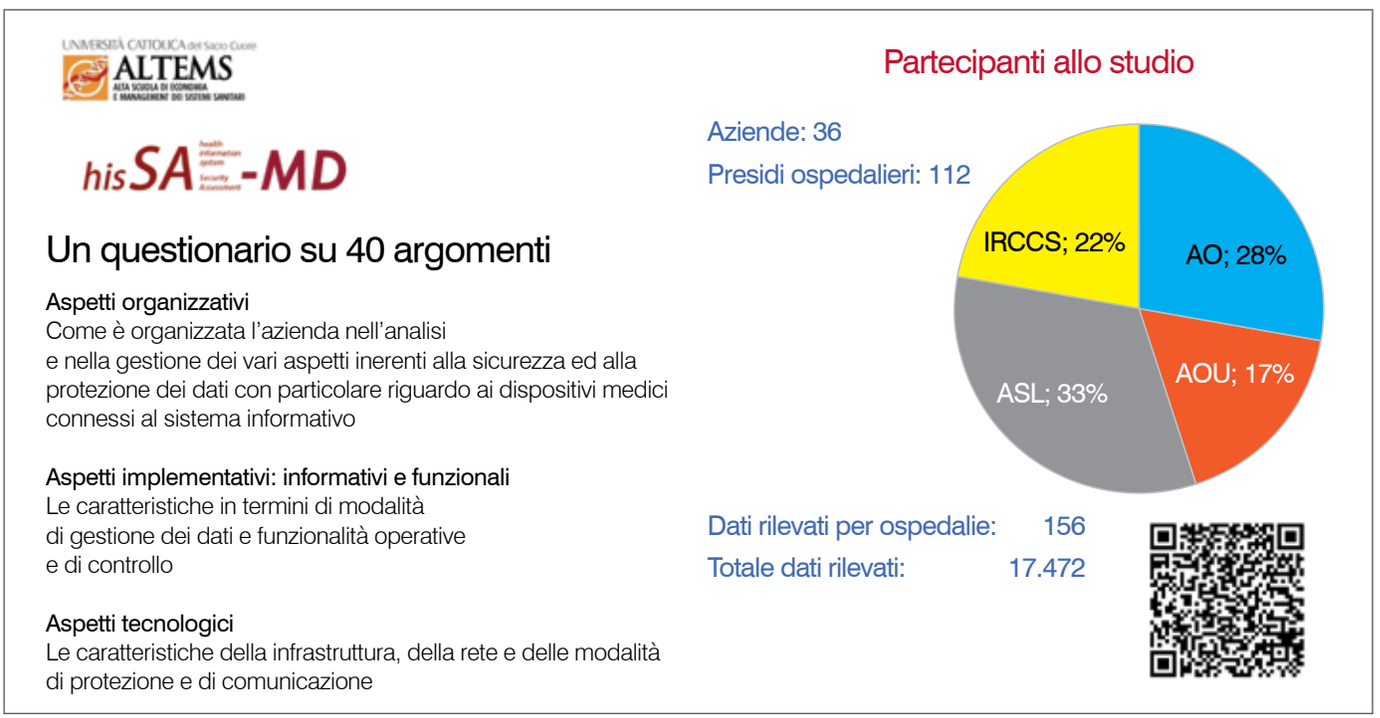


Figura 3: Indagine sulla sicurezza dei dispositivi medici connessi con i sistemi infromativi

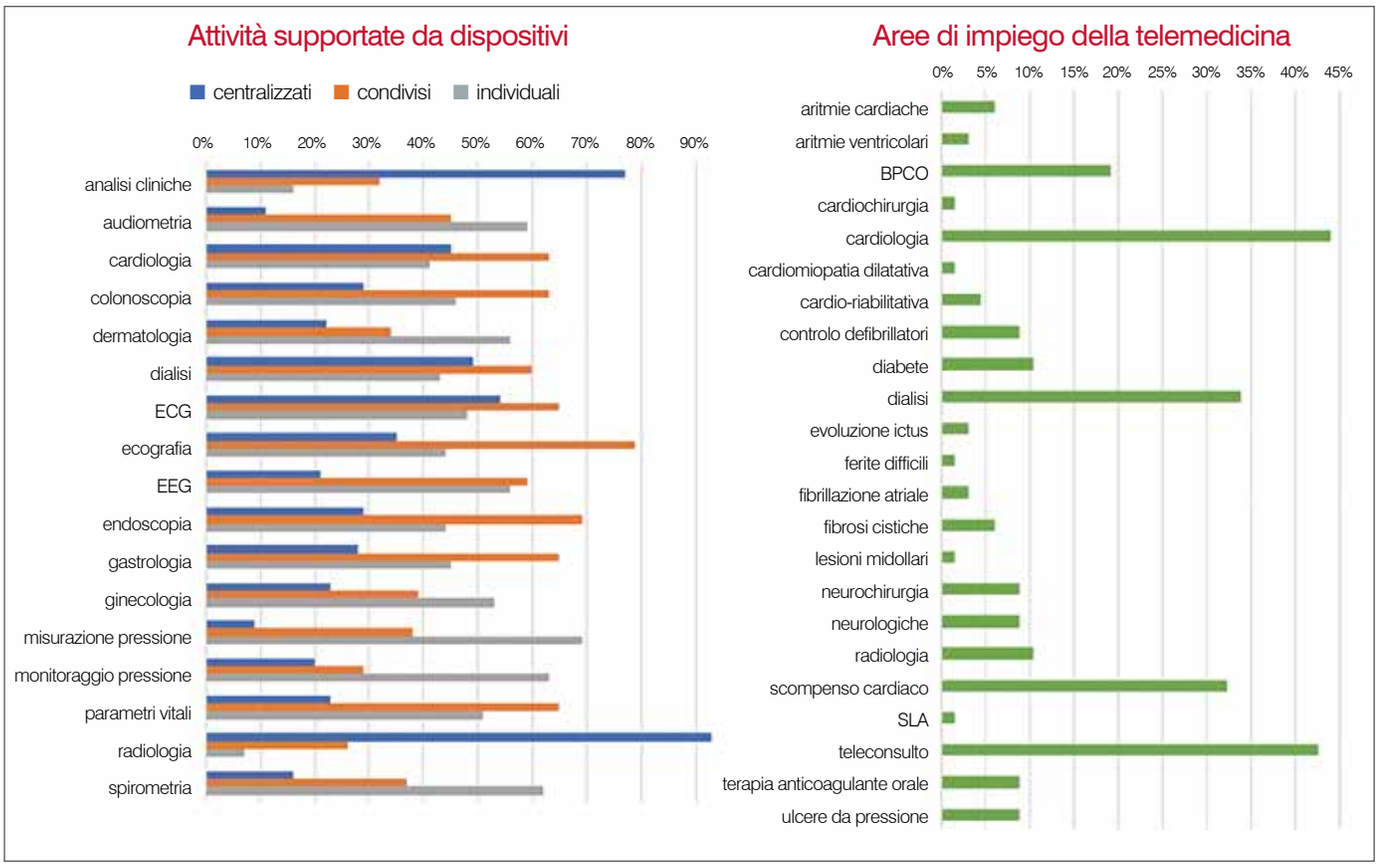


Figura 4: I principali ambiti di utilizzo dei dispositivi

laborazione formalizzata fra le funzioni responsabili della sicurezza del sistema informativo e quelle responsabili del rischio clinico.
Relativamente ai dispositivi, l'attenzione agli aspetti di rischio e la gestione della sicurezza nei dispositivi (in particolar modo quelli condivisi ed individuali) sono di gran lunga inferiori rispetto a quanto presente nel sistema informativo.
Questa situazione è riscontrata relativamente tutte le tipologie di rischio analizzato. In particolare va evidenziato come la diversità dei prodotti e delle tecnologie, insieme alla non integrazione e modalità di gestione frammentata specialmente per quanto riguarda i dispositivi condividi ed individuali, renda molto alta la percentuale dei casi in cui si riscontra anche un forte rischio in termini di protezione dei dati personali, in termini di:

- assenza di procedure formalizzate a livello organizzativo circa le modalità di comportamento circa i dati stessi;
- assenza di procedure di verifica periodica del rischio;
- mancanza di controlli (a volte impossibili, stante la distribuzione logistica dei dispositivi e la loro non integrazione con il resto del sistema) per quanto riguarda la non diffusione di credenziali.

Questa minore attenzione dell'organizzazione verso i dispositivi condivisi ed individuali si traduce anche in maggiori rischi sotto il profilo informativo, funzionale e tecnologico.

Aspetti informativi

I dati acquisiti dai dispositivi condivisi che vengono integrati nel sistema informativo sono in quantità nettamente inferiore di quanto avviene per i dispositivi centralizzati, per giungere ad una percentuale trascurabile nel caso di dispositivi individuali. Parallelamente rimane alta la percentuale dei dati che rimangono registrati permanentemente sui dispositivi condivisi e individuali.
Questi aspetti determinano sia limitazioni in termini di disponibilità di informazioni complete a supporto delle attività cliniche in tutta la struttura, sia rischi in termini di protezione dei dati, stante la bassa integrazione dei dispositivi condivisi e individuali con il sistema informativo e la loro intrinsecamente maggiore vulnerabilità in termini di gestione e controllo.
Inoltre, sui dispositivi condivisi ed individuali sono poco presenti meccanismi di associazione sicura dell'identità del paziente ai dati rilevati e funzionalità in grado di evidenziare situazioni di allarme.

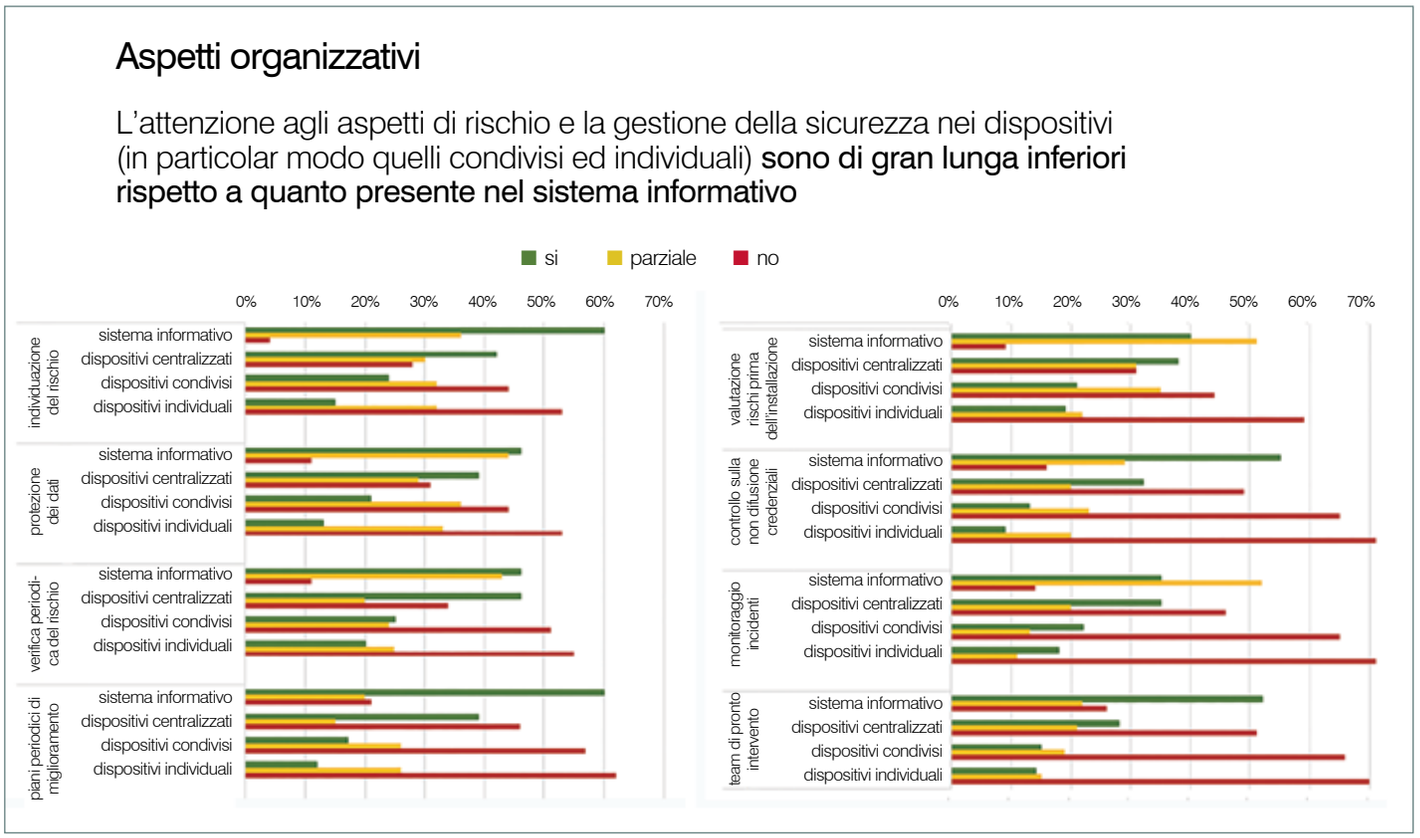


Figura 5: Gli aspetti organizzativi

Aspetti funzionali

I dispositivi condivisi ed individuali presentano elevati livelli di rischio nella gestione delle attività e nella protezione e sicurezza dei dati, in particolare:

- è molto alta (superiore al 60%) l'assenza di meccanismi di autenticazione e di abilitazione centralizzata nell'accesso;
- è molto alta (superiore al 70%) l'assenza di meccanismi di log delle attività effettuate dagli utenti;
- sono praticamente assenti (meno del 15% dei casi) meccanismi in grado di tenere traccia della storia dei dati raccolti e di ripristinare versioni precedenti (questo unito al fatto che gran parte delle informazioni rimangono stabilmente registrate sul dispositivo).

Aspetti tecnologici

Per quanto riguarda le caratteristiche dell'infrastruttura:

- in oltre il 10% dei contesti non viene gestito un inventario dei componenti collegati alla rete (come sarebbe peraltro richiesto dalle normative AgID);
- la continuità di esercizio non è assicurata in circa il 15% dei casi ed è garantita solo per le aree critiche (Pronto soccorso, rianimazione, sale operatorie, etc.) in solo il 60% dei casi e solo per il sistema informativo ed i dispositivi centralizzati. Questa percentuale scende a meno del 20% dei casi per i dispositivi condivisisi ed a meno dell'8% dei casi per i dispositivi individuali.

Anche l'operatività dei dispositivi condivisi ed individuali presenta livelli di rischio più elevati:

- è molto alta (superiore al 55%) l'assenza di meccanismi per l'identificazione e la rimozione di software dannosi;
- è molto alta (superiore all'80%) l'assenza di protocolli protetti per la comunicazione sulla rete;
- è molto alta (ovvero poco controllata) la possibilità di comunicazione autonoma con l'esterno (ad esempio mediante modem locali), il che amplifica i rischi riscontrati in termini di assenza di meccanismi centralizzati di identificazione ed autenticazione.

CORRELAZIONE CON I FATTORI DI RISCHIO E IL MODELLO DI MATURITÀ PER LA SICUREZZA

Gli indicatori raccolti mediante il questionario sono stati correlati con le varie tipologie di rischio, classificate, secondo un approccio di Health Technology Assessment, in tre prospettive: sicurezza del paziente, protezione dei dati personali, aspetti economici, come in fig. 6.

Tenendo conto di questi vari aspetti è stato definito un modello di maturità in grado di rappresentare le modalità secondo cui l'azienda affronta le diverse problematiche inerenti alla sicurezza ed alla protezione dei dati nei dispositivi medici.

Simmetricamente rispetto alle tipologie di indicatori definiti, il modello si articola secondo le seguenti prospettive:

Figura 6: Correlazione tra le tipologie di rischio e le caratteristiche del sistema informativo

Prospettiva organizzativa

analizza le caratteristiche secondo cui è organizzata l'azienda dal punto di vista della valutazione, del controllo e della gestione dei rischi, sia a livello preventivo che in caso di incidenti.

Prospettiva implementativa, suddivisa in aspetti funzionali ed aspetti informativi

analizza le caratteristiche del contesto sotto il profilo delle operatività attualmente implementate nel supporto ai processi assistenziali, sia dal punto di vista funzionale che sotto il profilo della gestione e della protezione dei dati.

Prospettiva tecnologica

analizza le caratteristiche strutturali ed operative della infrastruttura tecnologica di supporto ai dispositivi medici nell'ambito del sistema informativo.

Per ogni prospettiva sono stati definiti quattro livelli - dal valore 0 al valore 3 secondo una scala crescente, da uno stadio preliminare a quello più avanzato e, di conseguenza, più maturo e completo in termini di sicurezza.
Molto sinteticamente, gli scenari corrispondenti ad i singoli livelli sono descritti nel seguito.

Livello 0 - Preliminare

Denota un contesto in cui le problematiche inerenti all'integrazione dei dispositivi medici con il sistema informativo e di supporto all'operatività nonché la protezione dei dati sono ancora affrontate separatamente nei vari contesti operativi, secondo criteri e soluzioni frammentate per i singoli dispositivi (essenzialmente quelli centralizzati), senza una visione integrata nell'azienda e delle diverse prospettive del rischio.

Livello 1 - Iniziale

Denota un contesto in cui l'azienda dimostra sensibilità e di aver cominciato ad affrontare in modo organico le problematiche inerenti all'integrazione e la protezione dei dati nel collegamento con i dispositivi medici.
Le conseguenti caratteristiche operative sono però ancora ancora ad uno stato iniziale, circoscritte ad un numero limitato di settori e di processi, principalmente per quanto riguarda i dispositivi centralizzati. L'infrastruttura tecnologica presenta fattori di elevata criticità.

Livello 2 - Intermedio

Denota un contesto in cui l'azienda dimostra di affrontare in modo organico le problematiche inerenti alla sicurezza ed alla protezione dei dati nella gestione dei dispositivi medici integrati con il sistema informativo.

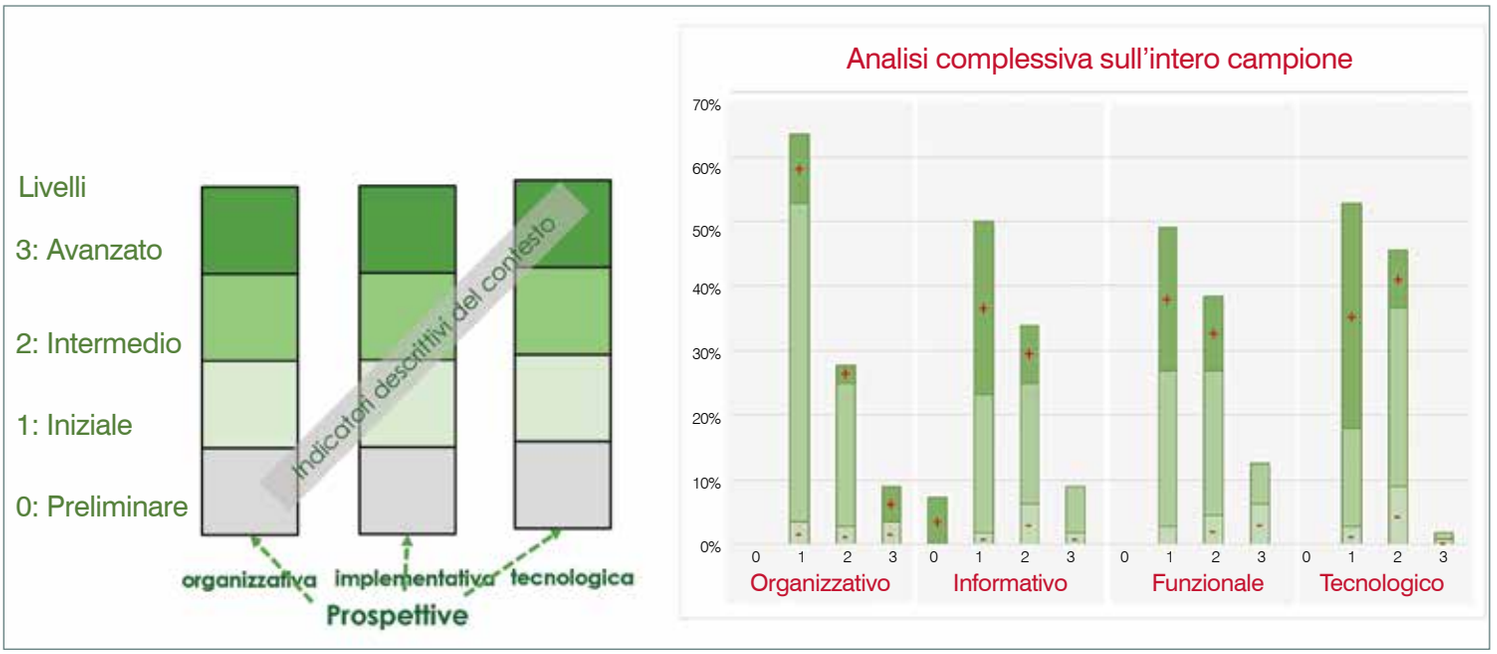


Figura 7: Maturità nella gestione della sicurezza nei dispositivi medici secondo le diverse prospettive

L'organizzazione della gestione è omogenea e sono presenti caratteristiche implementative in grado di contribuire alla sicurezza dei dati e dei processi anche mediante la centralizzazione di informazioni, regole e funzionalità.
Il contesto presenta tuttavia ancora fattori di rischio non trascurabili: le attività di gestione e controllo sono focalizzate sui dispositivi centralizzati e -non totalmente- sui dispositivi condivisi, una elevata percentuale di dati permane stabilmente sui dispositivi condivisi (senza particolari misure di protezione) e l'infrastruttura di comunicazione presenta ancora alcuni aspetti di criticità.

Livello 3 - Avanzato

Denota un contesto in cui l'azienda affronta in modo organico le problematiche inerenti alla sicurezza, tenendo in forte considerazione anche le problematiche relative al supporto integrato a processi clinici ed operando secondo un approccio propositivo, di monitoraggio, pianificazione e di continuo miglioramento.
La gestione dei dispositivi centralizzati e condivisi, ed -in parte- anche di quelli individuali avviene secondo criteri omogenei, sia pur a livello implementativo diverso nei diversi settori.
Sono presenti (sia pur a livello diverso nei vari contesti) caratteristiche implementative e procedure operative in grado di contribuire alla sicurezza dei processi ed alla protezione dei dati, anche mediante la centralizzazione di informazioni, regole e funzionalità di uso comune, e l'esistenza di meccanismi di protezione sui singoli dispositivi. L'infrastruttura tecnologica di comunicazione non presenta elementi di particolare criticità.
Sono inoltre presenti meccanismi proattivi per l'evidenziazione automatica di situazioni di rilevanza e per la prevenzione del rischio sia a livello funzionale che tecnologico.
I dati raccolti dai 112 ospedali partecipanti all'indagine sono stati analizzati secondo gli indicatori ed organizzati nell'ambito del modello di maturità. Mediante tale elaborazione si è ottenuta la classificazione dei livelli di sicurezza nelle strutture sanitarie come rappresentata in fig. 7.
Come evidenziato, la composizione del campione, sia in termini geografici che di tipologia di aziende sanitarie è rappresentativa della realtà nazionale. L'applicazione del modello di maturità rappresenta pertanto una fotografia ragionevolmente significativa del livello di sicurezza dei dispositivi sanitari nel contesto dei sistemi informativi delle aziende sanitarie italiane.
Va comunque considerato che le strutture che hanno partecipato all'indagine sono probabilmente caratterizzate da una maggiore sensibilità verso le problematiche della sicurezza. La percentuale delle strutture classificabili secondo livelli di minore maturità può pertanto essere, nella realtà, superiore a quella evidenziata dall'indagine. Il rapporto completo, con i risultati dell'indagine, gli indicatori, ed il modello di maturità è disponibile sul sito ALTEMS.

L'autore **FABRIZIO MASSIMO FERRARA**

Coordinatore del "Laboratorio ALTEMS sui sistemi informativi sanitari"