UNIVERSITÀ CATTOLICA del Sacro Cuore
ALTEMS
ALTA SCUOLA DI ECONOMIA E MANAGEMENT DEI SISTEMI SANITARI

hisSA health information system Security Assessment

Metodologia di analisi e modello di classificazione della sicurezza nei sistemi informativi sanitari secondo un approccio di Health Technology Assessment

Fabrizio Massimo Ferrara [1] – Americo Cicchetti [2]

[1] Coordinatore scientifico "Laboratorio sui sistemi informativi sanitari", ALTEMS
[2] Direttore ALTEMS

Con il contributo di:

- Massimo Casciello, Direttore Generale della "Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica" del Ministero della Salute
- Quirino Davoli, Responsabile dei Sistemi Informativi, ASL Roma-1
- Luca Giorgio, Ricercatore ALTEMS
- Sergio Pillon, Coordinatore della Commissione Tecnica Paritetica del Ministero della Salute per lo sviluppo della telemedicina nazionale
- Filippo Servello, Ricercatore ALTEMS
- Elena Sini, Direttore Sistemi Informativi Istituto Clinico Humanitas

ALTEMS Working paper

Versione 1.0 – 02.05.2017

Management Summary

Il sistema informativo di una azienda sanitaria 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.

In una tale visione, una valenza particolare assume la gestione della sicurezza, 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 i rischi, che –per le particolari caratteristiche del contesto sanitario- assumono una rilevanza particolare in quanto possono avere implicazioni anche sulla stessa salute del paziente.

Anche per quanto riguarda il profilo legale, vale sottolineare come le normative sulla privacy definiscano regole di ampio respiro, non circoscrivibili a singole attività o procedure, ma di rilevanza per tutte le attività dell'organizzazione e per tutti i componenti del sistema informativo in un contesto integrato di continuità di processo e di condivisione di informazioni.

Con questo obiettivo, viene proposta una metodologia per l'analisi complessiva della sicurezza del sistema informativo sanitario, secondo un approccio multidimensionale che coniuga le linee guida definite dai principali standard ed iniziative nel settore dell'ICT (sanitario e non) con le prospettive caratterizzanti l' Health Technology Assessment, tenendo ovviamente conto anche degli aspetti normativi, quali quelli relativi alla privacy.

Le caratteristiche -organizzative, strutturali ed implementative- dei sistemi informativi sono espresse mediante indicatori di validità generale ed indipendenti da specifiche soluzioni tecnologiche e/o di mercato che sono correlati con i diversi fattori di rischio, in modo da fornire alle singole aziende ed alle istituzioni uno strumento utilizzabile per analizzare lo stato attuale e definire piani evolutivi secondo le proprie esigenze e strategie.

In funzione di tali indicatori, è definito un modello di riferimento articolato in livelli, secondo cui classificare i sistemi informativi sanitari sotto il profilo della sicurezza nella sua globalità, anche in un'ottica di confronto e benchmarking.

Per la validazione ed il raffinamento della metodologia, il "Laboratorio sui Sistemi informativi Sanitari" dell' ALTEMS –l'Alta Scuola di Economia e Management dei Sistemi Sanitari dell'Università Cattolica del Sacro Cuore-, in collaborazione con la "Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica" del Ministero della Salute, ha condotto una indagine sui sistemi informativi, mediante la diffusione ad aziende sanitarie italiane pubbliche e private di un questionario sulle caratteristiche della propria organizzazione e del proprio sistema informativo.

Allo studio -i cui risultati principali sono inclusi in questo rapporto- hanno collaborato 46 aziende per un totale di 113 presidi ospedalieri, permettendo di ottenere una fotografia rappresentativa e significativa della realtà italiana, sia dal punto di vista geografico che della tipologia di organizzazioni.

Indice

Prefazione

I sistemi informativi per la gestione della persona nel SSN sono e saranno sempre più pervasivi.

D'altronde ciò non corrisponde solo alla esigenza di avere immediatamente informazioni per migliorare la diagnosi o cura ma anche per rendere sostenibile un SSN sempre più gravato dal dover assistere un gran numero di persone anziane con più patologie croniche. Pertanto i sistemi informatici dovranno integrarsi, espandendosi, sul territorio ed essere percorsi da notizie "certe ed affidabili". Questo consente una gestione efficiente, efficace e soprattutto economicamente sostenibile del SSN.

Parlare di sicurezza dei sistemi informativi sanitari non può quindi essere limitato solo agli aspetti tecnologici. Impedire accessi non autorizzati è il problema nel mondo della condivisione delle informazioni. Nel mondo sanitario non è l'unico, perché informazioni che riguardano lo stato biologico, così come immagini o come diagnosi, riguardano l'essere persona con i propri diritti di riservatezza, ma sono anche importanti per decidere opportunamente i processi di cura. Pertanto le notizie debbono fluire seguendo percorsi precisi ed essere disponibili solo a quei dipendenti del SSN che ne hanno bisogno rispettando il principio di necessità e non eccedenza. Ultimo aspetto è quello della qualità e tempestività delle informazioni. I sistemi debbono garantire di fornire notizie attendibili e con la giusta velocità. Pertanto la sicurezza nasconde più aspetti, e tutti assolutamente importanti.

I sistemi informativi hanno un impatto sulla salute, misurabile sia in termini di benessere fisico e sociale, sia in termini economici. L'introduzione dei sistemi informatici comporta sempre nuovi processi organizzativi ed impatto sui pazienti, dunque è necessario misurare e rendere confrontabili le soluzioni. L'approccio multidimensionale proprio dell' Health Technology Assessment, quindi, non è solo consigliabile ma si rivela assolutamente indispensabile per questo scopo.

Questo studio è un tentativo per cercare di comprendere l'esistente e per raggiungere soluzioni metodologiche, organizzative e tecnologiche condivise o condivisibili; insieme a tutti i componenti del SSN, nessuno escluso.

Per ultimo non vanno dimenticati i cittadini che vanno sempre ascoltati per comprendere se soluzioni ritenute dagli esperti assolutamente valide lo siano nella stessa misura per loro. Il SSN è degli italiani tutti.

Massimo Casciello
Direttore Generale
Direzione generale della digitalizzazione,
del sistema informativo sanitario e della statistica
del Ministero della Salute

1. L'esigenza di un approccio multidimensionale per la gestione della sicurezza e della privacy nei sistemi informativi sanitari

E' ormai ampiamente riconosciuto che in una 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 di assistenziale del paziente.

In una tale visione, una valenza particolare assume ovviamente la gestione della "sicurezza" (includendo in questo termine anche gli aspetti di privacy), 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.

La stessa norma ISO/IEC 27001 –inizialmente nata con un focus principalmente tecnologico- nelle sue più recenti versioni si è ampliata verso un approccio olistico di "sicurezza totale", che abbracci l'analisi e per quanto possibile la prevenzione di tutti i rischi aziendali. Sul sito ISO la norma viene infatti testualmente definita come "*requirements for an Information Security Management System (ISMS): a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process*".

Anche per quanto riguarda il profilo normativo, vale la pena di sottolineare come le disposizioni sulla Privacy definiscano regole di ampio respiro, non circoscrivibili a singole attività o procedure ma di rilevanza per tutte le attività dell'organizzazione. Il loro rispetto nell'ambito del sistema informativo, pertanto, richiede un approccio organico ed integrato che tenga conto di tutti gli aspetti in tutti i settori: dall'organizzazione dei dati, alle funzionalità, alle tecnologie.

In questa visione maggiormente strategica, anche le caratteristiche funzionali ed informative del sistema informativo costituiscono quindi elementi fondamentali e qualificanti ai fini della sicurezza e della gestione del rischio nell'azienda sanitaria.

In estrema sintesi l'obiettivo finale di un "sistema informativo sicuro" può essere individuato nella capacità 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 di rendere disponibili tutte le informazioni di potenziale rilevanza nei tempi e nei modi appropriati per le diverse esigenze. Includendo in questo scenario di completezza informativa non solo il rendere disponibili "passivamente" tutte le informazioni sul paziente, indipendentemente dal momento e dal settore in cui tali informazioni sono state raccolte, ma anche la capacità di svolgere un ruolo proattivo nei confronti dell'utente, evidenziando autonomamente situazioni di potenziale

rischio grazie alla correlazione delle informazioni stesse, sia sulla base di regole criteri già in uso nella pratica clinica (es- co-morbilità) che in base a più complessi algoritmi di knowledge discovery e business intelligence applicati alla medicina.

Il tutto secondo i ruoli e le abilitazioni dei vari utenti nel rispetto delle normative legate alla particolare natura dei dati trattati, coniugate con la necessità di poter gestire tempestivamente situazioni critiche e di emergenza.

In un tale scenario, la gestione della sicurezza nei sistemi informativi e la definizione di strategie evolutive che tengano conto sia delle possibilità connesse a nuovi modelli organizzativi e a nuove tecnologie(e dei rischi connessi), sia delle normative sempre più precise e stringenti si deve necessariamente basare su un approccio multi-dimensionale.

A questo scopo, la "tradizionale" analisi degli aspetti del sistema informativo in termini organizzativi, informativi, funzionali e tecnologici ([1]) può essere coniugata ed integrata con le prospettive proprie dell'approccio dall' Health Technology Assessment [2],[3], quali il rischio clinico[4], l'impatto sul paziente, l'aspetto economico, le implicazioni etiche, la rispondenza alle normative, etc.

Seguendo questo approccio, per disporre di termini di riferimento di validità generale, tali in modo da rendere possibile anche la classificazione ed il confronto secondo criteri omogenei, ci si può quindi basare su prospettive:

1 ISO/IEC 10746 "Information Technology - Open distributed processing – Reference model"
2 Ferrara, "ICT e HTA: il ruolo dell'HTA nella valutazione dei sistemi informativi sanitari"; IX congresso SIHTA, Ottobre 2016
3 Ferrara F.M., Cicchetti A., "I sistemi informativi e l'Health Technology Assessment", Progettare per la Sanità, Novembre 2016
4 Ferrara F.M., Pillon S. "Medicina Digitale – Sicurezza per il medico e per il paziente", Progettare per la Sanità, Settembre 2016

- le caratteristiche dei sistemi, descritte - secondo metodologie e standard propri dell'ICT- in modo da evidenziarne i vari aspetti in termini di organizzazione, struttura ed operatività, indipendentemente dalle specifiche soluzioni tecnologiche e di mercato;

- i requisiti di sicurezza nella sua accezione complessiva, articolati secondo le diverse prospettive suggerite dall'HTA, in modo da classificare le varie tipologie di rischio in funzione delle tipologie di conseguenze; dal punto di vista clinico, legale ed economico.

Integrando queste due prospettive, è possibile correlare le caratteristiche del sistema informativo con gli aspetti inerenti la sicurezza -intesi come tipologie di rischio- valutando lo stato attuale e definendo strategie ed iniziative secondo un approccio multidimensionale come evidenziato in figura, dove:

- **con "aspetti organizzativi"** ci si riferisce a come è organizzata l'azienda in relazione alla gestione delle problematiche inerenti la sicurezza nell'ambito della definizione, gestione ed evoluzione del sistema informativo;

- con "**aspetti strutturali**" si intendono le caratteristiche secondo cui è strutturato il sistema informativo nel suo complesso, in termini di aspetti architetturali e di validità generale per tutto il sistema, che possono contribuire nativamente ad aspetti di sicurezza e/o rendere più o meno agevole evoluzioni in questo ambito;

- con "**aspetti implementativi**" si considerano le caratteristiche del sistema informativo in termini di operatività e di funzionalità attualmente implementate nel supporto ai principali processi organizzativi ed assistenziali.

2. Metodo di lavoro

Sulla base di queste considerazioni, il "Laboratorio sui Sistemi informativi Sanitari" dell' ALTEMS –l'Alta Scuola di Economia e Management dei Sistemi Sanitari dell'Università Cattolica del Sacro Cuore-, in collaborazione con la "Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica" del Ministero della Salute, ha condotto uno studio finalizzato ad un duplice scopo:

- ottenere una "fotografia" omogenea delle caratteristiche dei sistemi informativi delle aziende sanitarie italiane, in termini di sicurezza, intesa in questa sua accezione "totale" del termine;
- proporre una metodologia per l' analisi e la classificazione dei sistemi informativi secondo "livelli di sicurezza", basati su un approccio olistico e su indicatori misurabili, indipendenti da specifiche soluzioni tecnologiche adottate.

Innanzi tutto è stato progettato un questionario, articolato in circa 40 voci, mediante le quali evidenziare le caratteristiche del sistema informativo sanitario, sotto il profilo organizzativo, strutturale e funzionale (evitando, si ripete, aspetti prettamente tecnologici e di mercato).

Per l'individuazione delle caratteristiche oggetto di analisi si è fatto riferimento alle indicazioni normative e di standardizzazione, ai casi di best-practices e di raccomandazioni da parte di istituti riconosciuti a livello internazionale, a quanto proposto sul mercato (principalmente, ma non esclusivamente, a livello italiano) ed ai principali trend evolutivi già attualmente riscontrabili (es. mobile health, percorsi assistenziali, continuità assistenziale sul territorio).

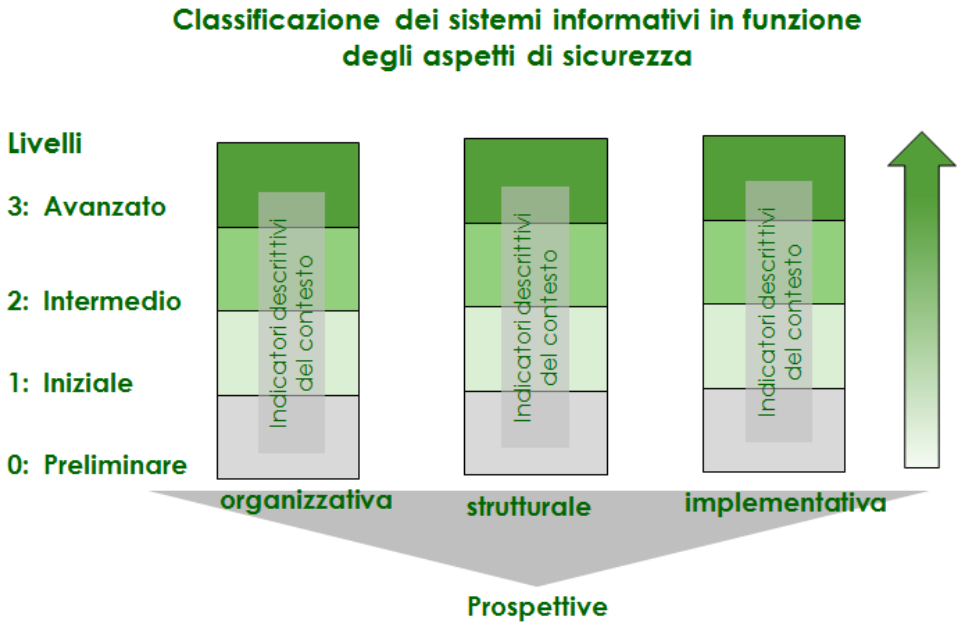
Il questionario è stato quindi diffuso ad aziende sanitarie di tutte le Regioni italiane, rappresentative dello scenario nazionale, chiedendo la loro collaborazione nella compilazione dello stesso, anche con l'aggiunta di informazioni ritenute significative. A tale scopo il questionario oltre a prevedere risposte "chiuse", comprendeva anche sezioni libere finalizzate per l'appunto ad una collaborazione attiva degli intervistati, mediante l'aggiunta di informazioni e suggerimenti.

Alla data di questo documento **sono stati ricevuti i contributi 46 aziende, per un totale di 113 ospedali,** che -come discusso nel seguito- rappresentano un campione rilevante e significativo della realtà nazionale.

Sulla base di questi contributi si è potuta innanzi tutto **delineare una fotografia del panorama attuale dei sistemi informativi sanitari**, relativamente ad un insieme di caratteristiche -organizzative, strutturali e funzionali- rilevanti sotto il profilo della completezza della continuità e -in definitiva- della qualità del supporto informatico disponibile.

In seconda istanza, a fronte dei contributi forniti dalle aziende partecipanti (anche in termini di annotazioni ed informazioni aggiuntive), gli argomenti oggetto del questionario sono stati raffinati e dettagliati fino a definire un insieme di indicatori -puntuali e misurabili- circa un insieme di caratteristiche dei sistemi informativi di rilevanza per le varie esigenze di sicurezza, come descritti nel § 6.

Sulla base di questi indicatori, è stato infine costruito un modello (descritto nel § 7) per la classificazione del grado sicurezza nei sistemi informativi, basato su quatto livelli crescenti, ognuno dei quali articolato secondo le prospettive organizzativa, strutturale ed implementativa.



Sulla base di questo quadro metodologico di riferimento, saranno in futuro possibili evoluzioni del modello, che includano ulteriori indicatori e livelli.

3. Gli aspetti relativi alla sicurezza nel sistema informativo

Nell'accezione di intendere la sicurezza del sistema informativo sanitario come la capacità dello stesso di fornire un supporto completo ed affidabile ai processi dell'azienda, prendendo spunto dall'approccio dell'Health Technology Assessment, gli aspetti inerenti la sicurezza sono articolati secondo diverse prospettive, dal punto di vista dei rischi e delle possibili conseguenze sul contesto organizzativo ed operativo del sistema sanitario come indicato nel seguito ([5],[6]):

3.1 Prospettiva inerente la sicurezza del paziente [7]

1. Identificazione sicura dell'individuo
2. Correttezza della terapia
3. Errore/incompletezza della comunicazione fra sanitari
4. Dimenticanza
5. Non considerazione di informazioni rilevanti
6. Non disponibilità di informazioni rilevanti
7. Errore nell'inserimento manuale dei dati
8. Tempestività delle azioni a fronte delle esigenze

3.2 Prospettiva etica e legale

1. Controllo nell'accesso alle informazioni
2. Identificabilità dell'autore di una operazione
3. Identificabilità dell'informazione ad una certa data
4. Perdita delle informazioni

3.3 Prospettiva inerente le normative

1. Rispondenza alle normative sulla privacy ed alle altre leggi applicabili
3. Completezza e correttezza di quanto attiene il debito informativo nei confronti degli organismi esterni

3.4 Prospettiva economica

1. Aumento dei tempi di degenza
2. Duplicazione di esami e/o attività
3. Non appropriatezza degli esami e/o attività
4. Tempo e risorse usate per eseguire una attività
5. Canoni di assicurazione
6. Costi legali anche relativamente al risarcimento di eventuali danni

[5] cfr F.M.Ferrara – S. Pillon "Medicina digitale: sicurezza per il medico e per il paziente", Progettare per la Sanità, Settembre 2016

[6] cfr National Data Guardian for Health and Care, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

[7] cfr anche Ministero della Salute, http://www.salute.gov.it/portale/temi/p2_6.jsp?id=250&area=qualita&menu=sicurezza

4. Gli aspetti sulle caratteristiche del sistema informativo

In quanto espressione delle diverse esigenze organizzative e scelte tecnologiche ed implementative i sistemi informativi presentano un grado molto elevato di diversità.

Per individuare dei termini di riferimento di validità generale indipendentemente da specifiche soluzioni tecnologiche ed in grado quindi descrivere in modo omogeneo le diverse realtà sono stati individuati alcuni indicatori in grado di parte l'individuazione di termini di riferimento omogenei è indispensabile per disporre di criteri di validità generale secondo i quali descrivere e confrontare i diversi scenari ad un livello concettuale indipendente da specifiche soluzioni implementative, ma al tempo stesso completo e non ambiguo in termini di requisiti e caratteristiche.

Per far ciò l'approccio seguito si è basato su alcune linee-guida di riferimento largamente diffuse:

a) ISO-ODP "Open distributed processing" che suggerisce l'adozione di quattro prospettive complementari, ma individualmente autonome ed auto-consistenti, per la descrizione del sistema: gli aspetti organizzativi, informativi, funzionali e tecnologici

b) ISO 12967 "Health Informatics Aystem Architecture", che -in accordo con questo riferimento metodologico-, propone un approccio incrementale di specifica ed un modello di riferimento, per quanto riguarda l'integrazione delle informazioni e la formalizzazione dei processi.

c) ISO-27001, la norma di riferimento per la sicurezza informatica, che nelle più recenti versioni si è ampliata verso un approccio di "sicurezza totale", per fornire un quadro metodologico complessivo, tale da abbracciare l'analisi la gestione e, per quanto possibile la prevenzione, di tutti i fattori di rischio.

d) HiMSS EMR Adoption Model, per la strutturazione di un insieme di livelli (fra loro cumulativi) nelle caratteristiche funzionali del sistema informativo, in relazione alla rilevanza e gli ambiti di utilizzo relativamente alle attività clinico-sanitarie.

Traendo spunto da queste linee guida, sono state individuate alcune caratteristiche del sistema informativo di possibile rilevanza ai fini della sicurezza, articolate secondo tre prospettive:

a) **prospettiva organizzativa**
Analizza le caratteristiche secondo cui è organizzata l'azienda in relazione alla gestione della sicurezza collegata con le funzionalità la gestione e l'evoluzione del sistema informativo.

b) **prospettiva strutturale**
Analizza le caratteristiche secondo cui è strutturato il sistema informativo nel suo complesso, in termini di aspetti architetturali che possono costituire nativamente ad aspetti di sicurezza e/o rendere più o meno agevole evoluzioni in questo senso

c) **prospettiva implementativa**

Analizza le caratteristiche del sistema informativo in termini di operatività e di funzionalità attualmente implementate nel supporto ai principali processi organizzativi ed assistenziali.

Nell'ambito di ognuna di queste prospettive sono individuate alcune caratteristiche di particolare rilevanza ai fini della prevenzione e gestione dei rischi e della sicurezza, nei termini espressi in precedenza.

Ovviamente, il sistema deve essere supportato da una infrastruttura tecnologica adeguata, sia sotto il profilo hardware che software. In questa sede, tuttavia, questi aspetti sono volutamente non approfonditi, in modo da mantenere l'analisi ad un livello tale da poter rappresentare un quadro di riferimento di requisiti e di caratteristiche di validità generale, implementabili con soluzioni e prodotti diversi anche in funzione dell'evoluzione delle tecnologie e del mercato.

4.1 Prospettiva organizzativa

Secondo i principi ormai acquisiti in tutti i sistemi di qualità, si sono considerati tre aspetti fondamentali nell'ambito della struttura organizzativa:

a) la sensibilità verso le problematiche
b) la strutturazione delle iniziative in un quadro organico di pianificazione e di valutazione
c) la gestione ed il monitoraggio del contesto di interesse in un'ottica di controllo e di miglioramento

Conseguentemente, si possono definire i seguenti gruppi di caratteristiche

4.1.1 Strutturazione organizzativa

Presenza nell'organigramma dell'azienda di una funzione preposta all'analisi ed alla definizione dei vari aspetti inerenti la sicurezza nell'ambito del sistema informativo

a) Esistenza di una funzione aziendale responsabile di individuare, pianificare e verificare gli aspetti rilevanti ai fini dei rischi e della sicurezza nell'ambito del sistema informativo secondo una visione complessiva che tenga di tutti gli aspetti rilevanti (organizzativi, informativi, funzionali e tecnologici).
b) Esistenza di procedure formali di collaborazione fra questa funzione e le funzioni aziendali responsabili della gestione del rischio clinico

4.1.2 Programmazione delle iniziative

Definizione periodica di piani integrati ed organici (comprensivi cioè di tutte le problematiche di rilevanza) per le iniziative inerenti la sicurezza e conseguente verifica dei risultati raggiunti

a) Redazione periodica di un documento programmatico circa tutti gli aspetti del sistema informativo rilevanti per la sicurezza nel suo complesso
b) Valutazione (assessment) periodica dello stato complessivo del sistema informativo in relazione alle varie problematiche rilevanti per la sicurezza e conseguente definizione del documento programmatico futuro.

4.1.3 Monitoraggio

Monitoraggio degli aspetti inerenti la sicurezza mediante procedure che diano evidenza e tengano traccia degli eventi di interesse e delle iniziative conseguentemente avviate.

4.1.4 Gestione delle abilitazioni

Abilitazione dei singoli utenti all'accesso al sistema ed all'esecuzione di tutte e sole le funzionalità necessarie, in accordo con le disposizioni normative e le regole aziendali. La presenza di una funzione aziendale unica e centralizzata per tutte le aree del sistema è un aspetto qualificante per garantire sia l'uniformità di applicazione, nonché l'adeguamento tempestivo e contestuale di tutti i settori all'evoluzione delle normative.

a) Esistenza di una funzione aziendale responsabile della definizione e della gestione delle credenziali di accesso individuali per tutte le procedure del sistema informativo

b) Esistenza di una funzione aziendale responsabile della definizione ed approvazione -eventualmente in collaborazione con i responsabili dei singoli settori- dei profili di abilitazione delle diverse tipologie di utenza nelle singole aree operative (ovvero delle specifiche funzionalità del sistema eseguibili dalle singole tipologie di utenza, nei diversi ruoli).

4.2 Prospettiva strutturale

Nell'ambito della prospettiva strutturale si individuano quelle caratteristiche che rappresentano le fondamenta secondo cui è organizzato l'intero sistema, rilevanti per tutte le applicazioni e quindi abbastanza stabili nel tempo e di non facile modificabilità.

In questa ottica, per quanto riguarda la sicurezza si individuano tre aree principali:
a) disponibilità ed affidabilità delle informazioni
b) accessibilità al sistema da parte degli utenti
c) tracciabilità delle attività effettuate dall'utenza

4.2.1 Disponibilità ed affidabilità delle informazioni

L'integrazione e la correlazione di tutte le informazioni relative al paziente costituisce un aspetto qualificante sia sotto il profilo della completezza e dell'affidabilità del supporto che il sistema informativo può fornire all'utenza nel processo clinico e decisionale (cfr [8]) che dal punto di vista dell'utilizzo delle informazioni stesse secondo regole comuni, includendo in questo contesto anche i meccanismi di protezione contro utilizzi non appropriati.

Secondo questo criterio, si definiscono gli indicatori seguenti:

a) Architettura complessiva del sistema informativo sanitario, classificabile in:

- architettura ERP completamente integrata (si precisa relativamente agli aspetti sanitari, non al sistema amministrativo)
- architettura basata su sistemi settoriali autonomi, interconnessi fra loro mediante meccanismi proprietari e/o standard

[8] Hospital implementation of health information technology and quality of care: are they related? http://www.bostonglobe.com/business/2016/05/16/partners-healthcare-new-computer-challenges-some-doctors-nurses/1I4QsWGjCJ97xFmUbcDbaJ/story.html?s_campaign=email_BG_TodaysHeadline&s_campaign=

- architettura mista, basata su un nucleo ERP per la gestione dei processi principali ed intersettoriali, collegato con applicazioni settoriali dedicate al supporto di singoli

b) Disponibilità di una struttura centrale (es. Clinical Data Repository[9]) potenzialmente in grado raccogliere ed integrare -a livello di dettaglio, non di solo documento, quindi diversa e complementare al Fascicolo Sanitario Elettronico- tutte le informazioni (correnti e storiche) sul paziente, rendendole disponibili a tutte le applicazioni che ne abbiano necessità, secondo regole e meccanismi centralmente definiti, anche in funzione delle normative vigenti.
La completezza (in termini di tipologia) delle informazioni integrate in tale repository ed il modello di organizzazione (possibilmente standard ed aperto) costituiscono aspetti rilevanti.

c) Disponibilità di una struttura centrale (es. Enterprise Imaging[10]), potenzialmente in grado raccogliere ed integrare tutte le immagini e dati multimediali sul paziente, rendendole disponibili a tutte le applicazioni che ne abbiano necessità, secondo regole e meccanismi centralmente definiti.
La completezza (in termini di tipologia) delle informazioni integrate in tale repository ed il modello di organizzazione (possibilmente standard ed aperto) costituiscono aspetti rilevanti

4.2.2 Accessibilità al sistema da parte degli utenti

I requisiti organizzativi di centralizzazione nella definizione e nel controllo delle abilitazioni all'accesso al sistema devono trovare riscontro in analoghe possibilità operative messe a disposizione dall'intero sistema informativo, valide a livello globale, per tutte le applicazioni.

a) Esistenza di un meccanismo di "Single sign on", che dia la possibilità di definire e gestire centralmente le credenziali degli utenti per tutto il sistema, assegnando ad ogni individuo un unico identificatore, con il quale accedere a tutte le procedure.

b) Esistenza di un ambiente mediante il quale definire e gestire i profili di abilitazione per tutte le aree del sistema e dell'organizzazione, definendo categorie di utenza ed associando a queste le opportune abilitazioni. (Nota: considerate le esigenze di mobilità e le specificità temporali, logistiche e clinico-operative dei diversi settori, non si ritiene qualitativamente significativa la centralizzazione delle associazioni dei singoli utenti ai diversi profili)

4.2.3 Tracciabilità delle operazioni

Riguardano sia quanto effettuato dagli utenti nel corso delle sessioni di lavoro che la storia dei valori assunti nel tempo dai singoli dati.

a) Registrazione di un giornale ("log") sugli accessi degli utenti al sistema e con i dati essenziali delle singole operazioni effettuate nell'ambito della sessione di lavoro. Il livello di dettaglio nella registrazione costituisce un elemento qualificante.

[9] cfr. https://en.wikipedia.org/wiki/Clinical_data_repository
[10] cfr. http://www.himss.org/library/clinical-informatics/enterprise-imaging

b) Registrazione, per ogni istanza della base dati, dello stato precedente ad ogni variazione effettuata e dell'autore della variazione stessa, in modo da poter risalire al valore assunto da ogni dato in qualsiasi momento precedente.

4.3 Prospettiva implementativa

Nell'ambito della prospettiva implementativa si individuano quelle caratteristiche attualmente presenti nel sistema informativo nell'ambito delle diverse procedure.

4.3.1 Tipologie e certificazione di documenti clinici registrati

La compilazione e registrazione di documenti clinici mediante il sistema informativo costituisce un aspetto qualificante sia ai fini della disponibilità che della affidabilità delle informazioni di interesse, contribuendo significativamente alla sicurezza del processo clinico.
Questo gruppo di indicatori descrive le tipologie di documenti clinici che sono compilati mediante il sistema informativo e registrati nell'ambito del patrimonio informativo del paziente.

In considerazione della loro rilevanza nei processi assistenziali e del volume delle informazioni gestite, si possono classificare le seguenti categorie principali:

a) Dati clinici di base, quali: anamnesi, diario clinico, prescrizioni e somministrazioni terapeutiche, ...

b) Dati assistenziali, quali: diario infermieristico, parametri vitali, requisiti assistenziali, ...

c) Referti, quali: analisi di laboratorio, radiodiagnostica, anatomia patologica, interventi operatori, cardiologia, esami ecografici, ...

La certificazione del documento mediante firma digitale costituisce un aspetto complementare, associabile ad ogni tipologia di informazioni registrata.
Oltre ai benefici logistici in termini di conservazione della documentazione, l'utilizzo della firma digitale riveste infatti un ruolo significativo nella sicurezza dei processi, sia garantendo al ricevente l'affidabilità del dato che evitando rischi di errore derivanti da trascrizioni manuali.

4.3.2 Completezza e continuità nel supporto ai processi

In questo ambito si analizza la capacità del sistema informativo di supportare con completezza e continuità interi processi sia inter- che intra-settoriali, dalla definizione iniziale alla esecuzione della prestazione, evitando discontinuità dovute a re-inserimenti manuali di informazioni già presenti nel sistema da altri settori e/o la necessità di complementi cartacei o verbali nelle comunicazioni fra gli interessati.

In considerazione della loro frequenza e potenziale criticità, si identificano -in prima istanza- i seguenti processi principali.

a) Percorso assistenziale dell'episodio nel suo complesso, mediante l'identificazione univoca del paziente e dell'episodio stesso con lo stesso codice identificativo in tutte le sue fasi: dalla lista di attesa, alla eventuale pre-ospedalizzazione, al ricovero (eventualmente a seguito di un accesso di emergenza), alla post-ospedalizzazione.

b) Prescrizione e somministrazione delle terapie
c) Processi -anche inter-settoriali- di erogazione di prestazioni e consulenze dal momento della richiesta, alla programmazione, alla esecuzione e refertazione, quali: esami di laboratorio, esami di diagnostica per immagini, esami ecografici, esami di anatomia patologica, consulenze ed esami cardiologici, consulenze ed esami ginecologici, consulenze ed esami oncologici, ...
d) Processo chemioterapico

4.3.3 Utilizzo di meccanismi per il riconoscimento automatico dell'individuo

Il riconoscimento sicuro dell'individuo costituisce uno dei principali elementi di rischio dal punto di vista dell'appropriatezza e della correttezza del trattamento praticato, specialmente se invasivo e/o di potenziale rischio per il paziente stesso.
Caratteristica qualificante è pertanto l'utilizzo di meccanismi automatici per il riconoscimento del paziente (RFID, braccialetto, etc.) nell'ambito di diversi eventi critici, quali: all'atto dei prelievi, alla somministrazione della terapia, al momento delle trasfusioni, durante i trattamenti chemioterapici, al check-in operatorio, durante la permanenza in Pronto Soccorso, ...

4.3.4 Supporto alle comunicazioni fra operatori

Il passaggio di informazioni, anche informali e non necessariamente parte della documentazione clinica- fra gli operatori coinvolti nella cura del paziente costituisce un momento di particolare criticità (cfr hand-over, [11]).
E' quindi rilevante la presenza di funzionalità in grado di supportare la collaborazione e scambi di informazioni anche informali (non parte della cartella clinica) fra gli operatori coinvolti nella cura e nell'assistenza al paziente

4.3.5 Proattività del sistema

Individua la capacità del sistema di evidenziare autonomamente situazioni di allarme e/o potenziale rilevanza, senza bisogno di una interrogazione specifica da parte dell'utente.
Fra i processi e gli eventi di maggiore criticità: situazioni di potenziale infezione ospedaliera, valori critici nei risultati di esami di laboratorio ([12]), valori critici nei parametri vitali, incompatibilità relativamente alla terapia, fattori di rischio e/o fragilità, resistenze ad antibiotici, ...

4.3.6 Affidabilità dell'infrastruttura

Definisce la capacità del sistema informativo nel suo complesso (infrastruttura hardware, dati, procedure) di assicurare la continuità del supporto ai processi, anche mediante una configurazione di disaster recovery.

[11] cfr WHO- Joint Commission http://www.who.int/patientsafety/solutions/patientsafety/PS-Solution3.pdf
[12] cfr Joint Commission http://www.macoalition.org/Initiatives/docs/CTRgriswold.pdf
Joint Commission "Critical Access Hospital National Patient Safety Goals", http://www.jointcommission.org/assets/1/6/2015_NPSG_CAH.pdf

5. L'indagine sulle caratteristiche dei sistemi informativi sanitari

5.1 Obiettivi e metodo di lavoro

A partire dal settembre 2016 il Laboratorio sui Sistemi informativi Sanitari dell' ALTEMS –l'Alta Scuola di Economia e Management dei Sistemi Sanitari dell'Università Cattolica del Sacro Cuore-, con la collaborazione della "Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica" del Ministero della Salute, ha avviato uno studio sui sistemi informativi delle aziende sanitarie italiane, con tre obiettivi;

a) ottenere una fotografia delle caratteristiche qualificanti dei vari sistemi sotto il profilo organizzativo, strutturale e funzionale, secondo criteri omogenei, indipendenti soluzioni di mercato adottate e tali quindi da poter essere condivisi quali termini di riferimento comuni;

b) dettagliare, anche sulla base dei contributi ricevuti mediante i questionari compilati, un insieme di indicatori -puntuali e misurabili- circa alcune caratteristiche dei sistemi informativi sanitari di particolare rilevanza ai fini della sicurezza e, più in generale, della qualità del supporto informatico disponibile alle attività cliniche ed assistenziali.

b) proporre, sulla base degli indicatori un modello per la classificazione in livelli del livello di sicurezza complessivo del sistema informativo.

Lo studio è stato condotto mediante un questionario sulla organizzazione delle aziende e sulle caratteristiche dei sistemi informativi sanitari secondo i criteri descritti nel precedente capitolo 4, che è stato diffuso fra le aziende sanitarie -pubbliche e private- di tutte le regioni italiane.

Per ogni argomento, il questionario prevedeva sia risposte chiuse che la possibilità di commenti e descrizioni aggiuntive, considerate dall'interlocutore utili per circostanziare meglio i singoli argomenti.

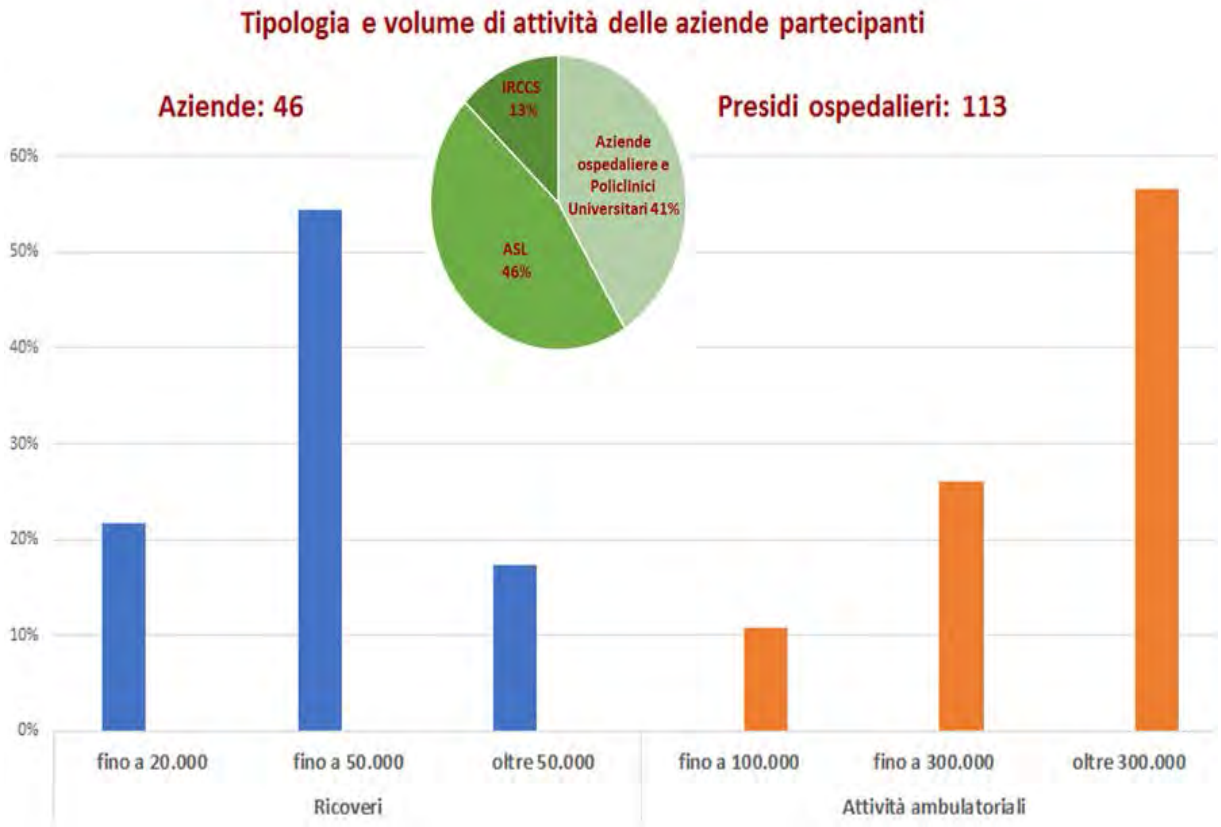
Grazie a tali contributi aggiuntivi, le caratteristiche inizialmente individuate sono state migliorate e dettagliate, consentendo la definizione degli indicatori e della struttura metodologica descritti nel seguito.

5.2 Caratteristiche delle aziende sanitarie partecipanti allo studio

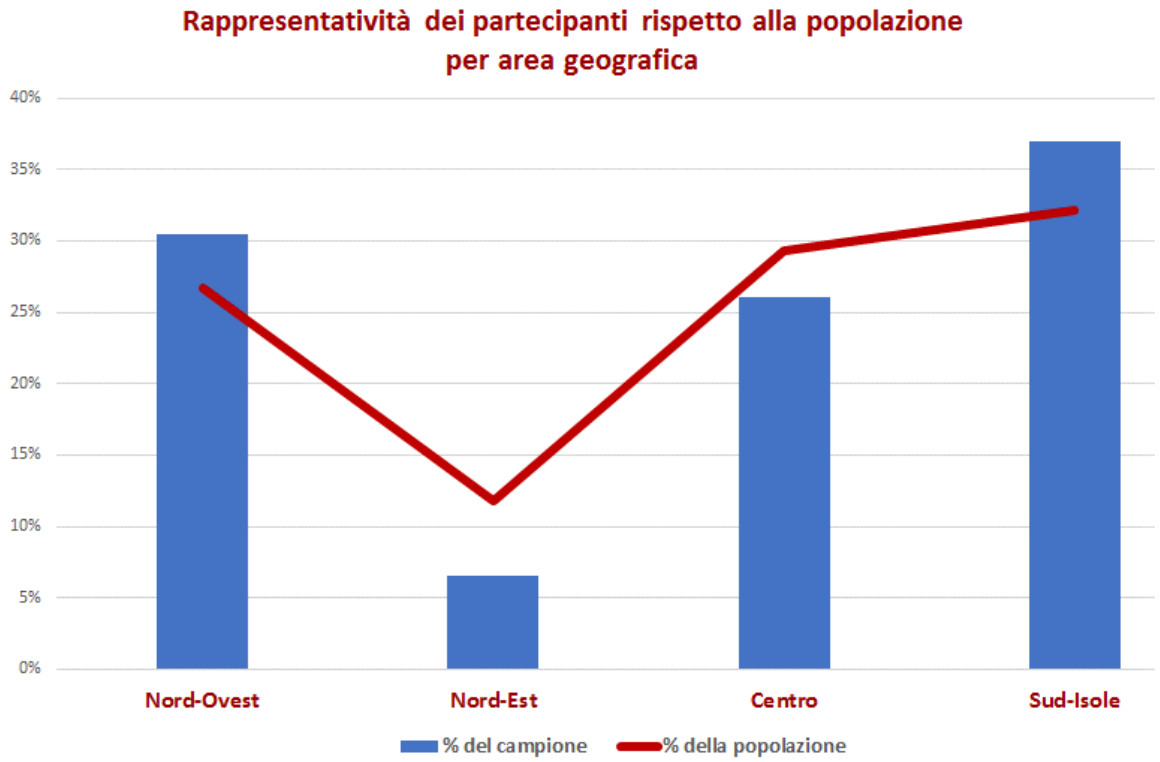
Alla data attuale, hanno collaborato allo studio un totale di 46 aziende sanitarie per un totale di 113 presidi ospedalieri.

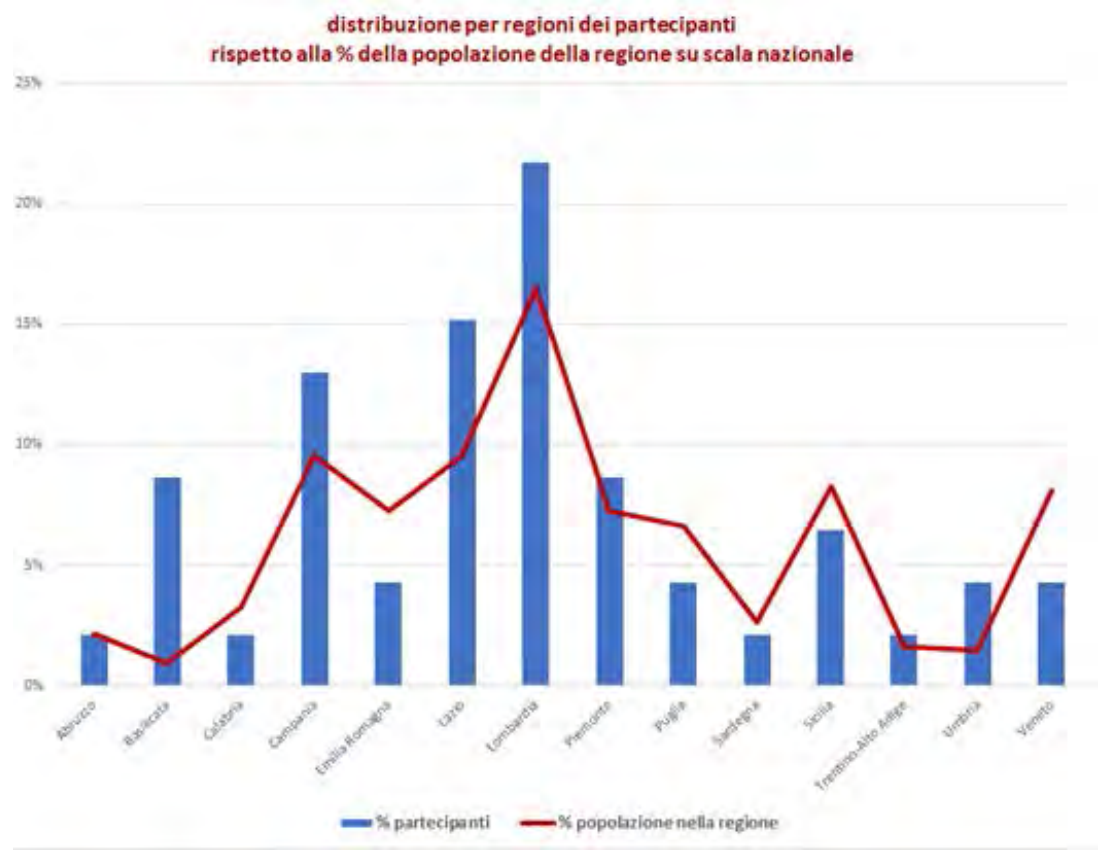
Come rappresentato nel seguito, l'insieme dei partecipanti costituisce un campione significativo e rappresentativo dello scenario nazionale, sia dal punto di vista geografico che di tipologia di organizzazioni sanitarie, tale da consentire una analisi scientificamente valida.

Lo studio è ancora aperto[13] in modo da consentire la raccolta di ulteriori contributi.

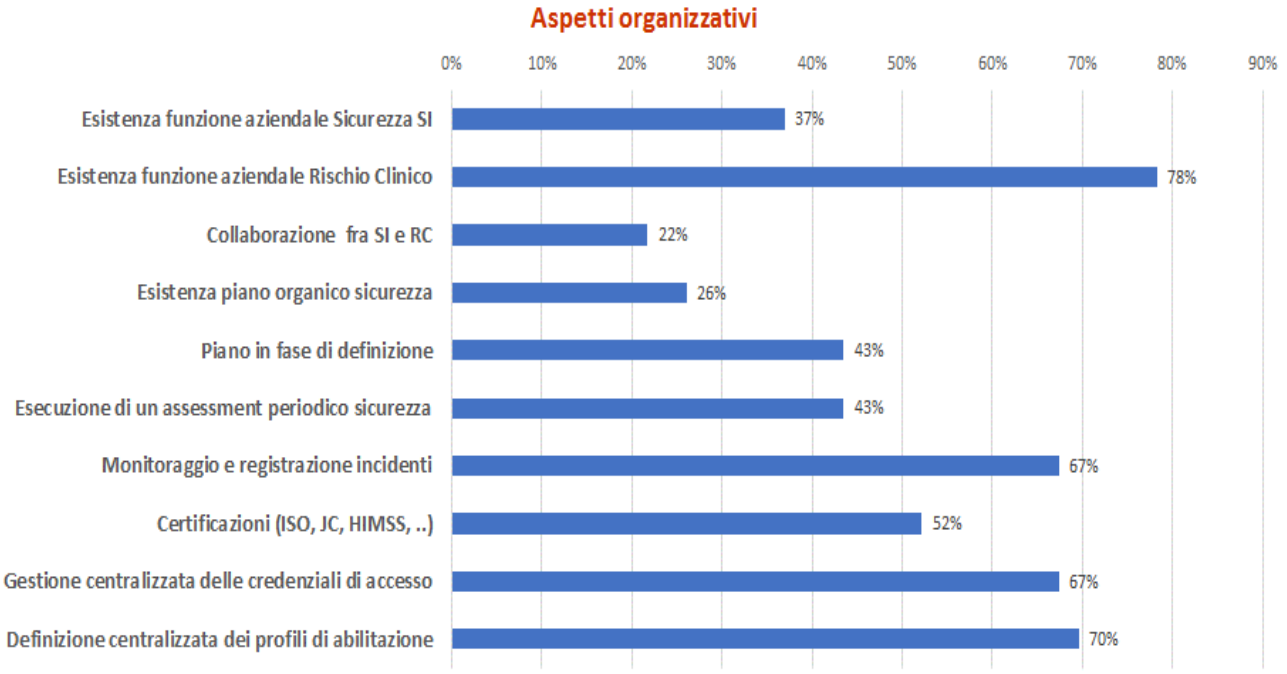


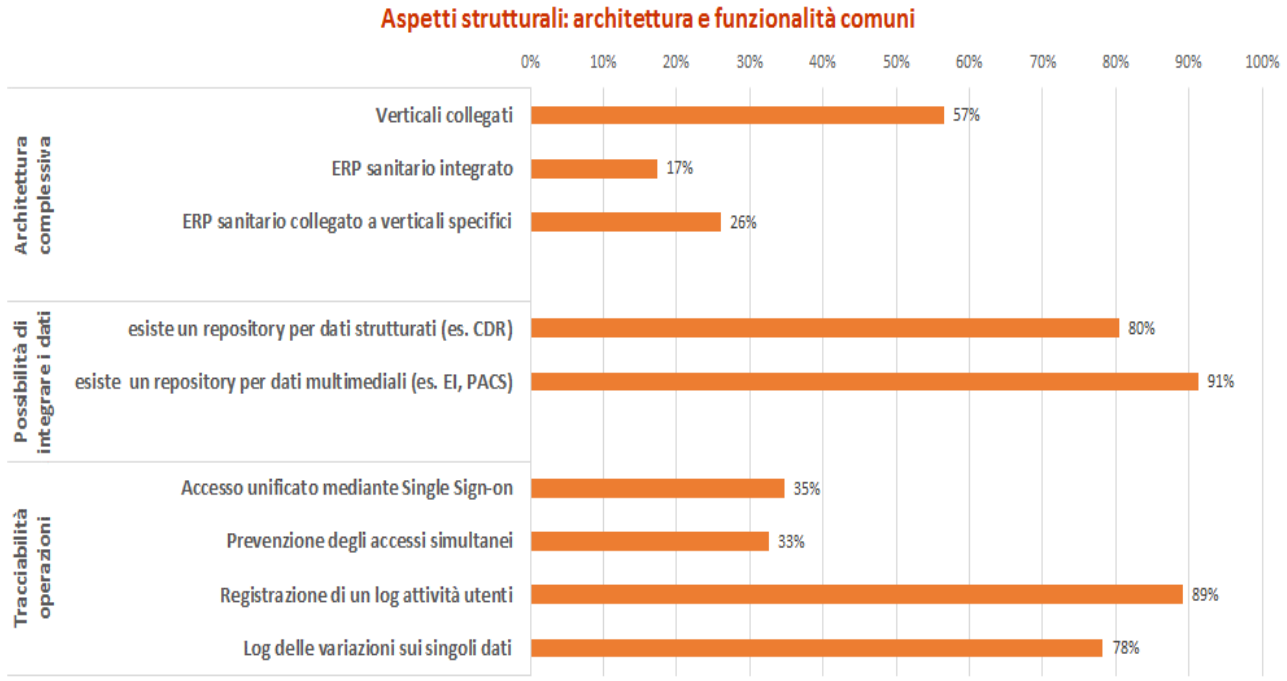
[13] Il questionario è compilabile on-line sul sito https://www.surveygizmo.com/s3/2743353/Livello-di-sicurezza-dei-sistemi-informativi-sanitari


Rappresentatività dei partecipanti rispetto alla popolazione per area geografica
40%
35%
30%
25%
20%
15%
10%
5%
0%
Nord-Ovest
Nord-Est
Centro
Sud-Isole
% del campione
% della popolazione


distribuzione per regioni dei partecipanti rispetto alla % della popolazione della regione su scala nazionale
25%
20%
15%
10%
5%
0%
Abruzzo
Basilicata
Calabria
Campania
Emilia Romagna
Lazio
Lombardia
Piemonte
Puglia
Sardegna
Sicilia
Trentino-Alto Adige
Umbria
Veneto
% partecipanti
% popolazione nella regione

5.3 Risultanze sui sistemi informativi analizzati






Aspetti implementativi: servizi e funzionalità attualmente disponibili
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Dati clinici registrati
Anamnesi
48%
39%
Diario clinico
30%
43%
Terapie
33%
48%
Dati infermieristici
28%
37%
Parametri vitali
24%
41%
Referti laboratori
93%
4%
Referti radiodiagnostica
91%
7%
Referti operatori
70%
28%
Consulenze
61%
26%
Altri documenti clinici
20%
4%
Percentuale dati registrati sul totale
fino a 40%
37%
fino a 65%
24%
fino a 85%
13%
oltre 85%
7%
Certificazione
Utilizzo della firma digitale (essenzialmente referti)
80%
15%
Registrazione del consenso informato
22%
28%
Continuità dei processi, dalla richiesta alla refertazione
Ricovero
78%
13%
Terapie
37%
33%
Esami di laboratorio
87%
7%
Esami di Radiodiagnostica
89%
7%
Interventi operatori
67%
17%
Cardiologia
48%
22%
Ginecologia
39%
22%
Oncologia
50%
26%
Altri processi
9%
Proattività
Meccanismi di riconoscimento individuo
48%
Supporto a comunicazioni informali
28%
Esistenza di allarmi automatici
48%
Configurazione di disaster recovery
43%
diffusione significativa
diffusione ridotta
% sul totale

6. Proposta di un set di indicatori per la descrizione delle caratteristiche del sistema informativo

6.1 Criteri

Come descritto in precedenza il questionario compilato dalle aziende che hanno partecipato allo studio era articolato in una serie di argomenti relativi alle caratteristiche del sistema informativo sanitario, prevedendo in ogni caso sia risposte chiuse che la possibilità di commenti e descrizioni aggiuntive, considerate dai partecipanti utili per circostanziare meglio i singoli argomenti.

Grazie a tali contributi aggiuntivi, le caratteristiche inizialmente individuate sono state formalizzate e dettagliate, fino alla definizione di un set di indicatori misurabili, in grado di evidenziare le caratteristiche di un sistema informativo sanitario, secondo criteri omogenei ed indipendenti dalle specifiche soluzioni tecnologiche adottate.

Al fine di rendere più oggettivo e misurabile il processo di analisi, per quanto possibile gli indicatori sono di natura binaria: “si” / “no”.

Va tuttavia considerato che -con esclusione di alcune informazioni ed alcuni processi fondamentali, di rilevanza nel processo di cura di un qualsiasi paziente- le diverse strutture presentano caratteristiche organizzative e cliniche diverse, che si traducono anche in una diversa rilevanza all’interno della struttura dei singoli processi e delle singole informazioni cliniche.

Simili diversità di possono riscontrare anche all’interno della stessa azienda, specialmente se di grandi dimensioni e multidisciplinare. In tali contesti, il livello di supporto e di utilizzo del sistema informativo raramente si evolve in modo continuo ed omogeneo contemporaneamente in tutta la struttura. I vari settori presentano infatti caratteristiche ed esigenze diverse, dovute alle diverse patologie trattate con le conseguenti differenze dal punto di vista clinico, organizzativo ed anche culturale, sia negli operatori che nei pazienti (a puro titolo di esempio, si pensi alla diversità delle procedure e dei modelli necessari per un paziente anziano affetto da co-morbilità croniche e poco collaborativo, rispetto a quanto invece richiesto a seguito di una frattura riportata da uno sciatore ventenne).

L’applicazione, indifferenziata, di indicatori binari (si/no) a tutto il sistema nel suo complesso non riuscirebbe pertanto a fornire un quadro veritiero della situazione effettiva, né per quanto riguarda la possibilità di confronto fra contesti diversi né dal punto di vista dell’aiuto alle singole aziende nella individuazione di percorsi evolutivi ed obiettivi di miglioramento in funzione delle proprie caratteristiche e strategie specifiche.

In alternativa, aumenterebbe significativamente il numero dei livelli di classificazione complessiva, che risulterebbero diversi l’uno dall’altro soltanto per aspetti di dettaglio, scarsamente significativi ai fini di analisi e benchmarking.

Per mantenere livelli di classificazione proposti di validità generale e basati sulle caratteristiche qualitative e non quantitative del sistema (in modo da facilitare il

confronto e la pianificazione), consentendo al tempo stesso di evidenziare diversi gradi di implementazione, ove applicabile gli indicatori sono complementati da indici qualitativi mediante i quali viene specificata la **diffusione** e la **rilevanza** nell'azienda della specifica caratteristica espressa dall'indicatore.

Con **diffusione** si intende il livello raggiunto nell'implementazione della caratteristica di interesse all'interno della struttura, espresso qualitativamente in termini di percentuale rispetto al totale, come indicato nella seguente tabella.

Indice di diffusione		% rispetto al totale degli elementi di interesse
A+	Molto alto	superiore ad 85%
A	Alto	fino a 85%
B	Medio	fino a 65%
C	Basso	fino a 35%
C-	Molto basso	inferiore a 10%

Esempio:
Ad esempio, la diffusione dell'indicatore "richiesta informatica per esami di laboratorio" è la percentuale del numero di richieste per esami di laboratorio effettuate mediante il sistema informativo rispetto al numero complessivo di richieste per esami di laboratorio effettuate nella organizzazione.

Sempre per la diversità delle esigenze cliniche ed organizzative fra le diverse strutture sarebbe altrettanto fuorviante, allo scopo di mantenere ragionevolmente contenuto il numero di indicatori descrittivi, alcune caratteristiche sono espresse in forma aggregata senza elencare tutte le possibili specializzazioni. Ad esempio, è definito un solo indicatore "diffusione nella registrazione di dati clinici" piuttosto un elenco di indicatori ognuno dei quali relativo ad un possibile documento di interesse.

Un tale livello di aggregazione sarebbe tuttavia troppo generico ed elevato per rappresentare i diversi contesti. Per raggiungere un livello di rappresentatività più significativo, questi parametri sono declinati secondo una "**classe di rilevanza**", mediante il quale stabilire dei sotto-insiemi rilevanti nello specifico contesto dell'azienda.

Classe di rilevanza		% rispetto al totale dei casi (pazienti)
A	Alta	oltre 70%
B	Media	fino a 70%
C	Bassa	fino a 30%

Esempio:
Ad esempio, l'indicatore "diffusione nella registrazione dei dati clinici" è dettagliato secondo tre sotto-indicatori, ognuno relativo ad una classe di rilevanza dei dati clinici gestiti.

	Classi di rilevanza dei dati gestiti	*Indice di diffusione della registrazione informatica*
A	*Dati clinici di alta rilevanza (oltre il 70% del totale dei casi gestiti)*	
B	*Dati clinici di media rilevanza (fino al 70% del totale dei casi gestiti)*	
C	*Dati clinici di bassa rilevanza (fino al 30% del totale dei casi gestiti)*	

6.2 Indicatori relativi alla prospettiva organizzativa

O1 Presenza di una funzione aziendale preposta alla sicurezza nel sistema informativo nel suo complesso, ovvero che tenga conto di tutti gli aspetti di rilevanza (organizzativi, funzionali, informativi e tecnologici) secondo le diverse prospettive di rischio.

O2 Collaborazione istituzionalizzata fra la funzione aziendale preposta alla sicurezza nel sistema informativo e quella preposta alla gestione del rischio clinico

O3 Definizione periodica di piani di attività organici, relativi alla sicurezza nel sistema informativo nel suo complesso, per tutti gli aspetti di rilevanza secondo le diverse prospettive di rischio

O4 Verifica periodica dello stato della sicurezza nel sistema informativo mediante momenti formali di assessment rispetto in funzione di quanto definito nel piano e di eventuali ulteriori criticità evidenziate nel periodo

O5 Esistenza di una procedura formalizzata di monitoraggio del sistema e di registrazione degli incidenti

O6 Gestione, sulla base della pratica quotidiana e del monitoraggio, di un "libro bianco" relativo a possibili correzioni e/o migliorie apportabili al sistema, tenute in considerazione al momento della redazione del piano

O7 Presenza di una funzione aziendale preposta al rilascio ed alla gestione delle credenziali di abilitazione all'accesso al sistema informativo

O8 Presenza di una funzione aziendale preposta alla definizione -eventualmente in collaborazione con i responsabili dei singoli settore- dei profili e delle regole di abilitazione delle diverse tipologie di utenti nell'utilizzo delle varie procedure del sistema informativo.

O9 Definizione ed utilizzo di vocabolari e codifiche uniformi (e possibilmente aderenti a standard e nomenclatori diffusi) per l'individuazione di attività, dati clinici, e -in generale- concetti di rilevanza ed interesse comune, sia all'interno della struttura che -potenzialmente- anche nelle interazione con altre organizzazioni.

O10 Presenza di criteri per la regolamentazione ed il controllo dell' uso di dispositivi personali da parte di operatori sanitari e di pazienti nell'ambito dei processi assistenziali supportarti dal sistema informativo.

6.3 Identificatori relativi alla prospettiva strutturale

S1 Presenza di un repository centralizzato (es. Clinical Data Repository) nel quale **integrare tutte le informazioni cliniche, assistenziali ed operative** relative ai pazienti, ad un livello di dettaglio tale da renderne possibile l'accesso e l'utilizzo operativo da parte delle varie procedure (e.g. non solo documenti integrati) secondo criteri e regole unificate, rispondenti alle normative ed alle procedure aziendali. La rispondenza di tale repository a modelli standard ed a criteri di apertura costituisce un elemento aggiuntivo qualificante.

S2 Presenza di un repository centralizzato (es. Enterprise Imaging, PACS aziendale, etc.) nel quale **integrare tutte le immagini ed i dati multimediali** relativi ai pazienti, rendendone possibile l'accesso e l'utilizzo operativo da parte delle varie procedure secondo criteri e regole unificate, rispondenti alle normative ed alle procedure aziendali. La rispondenza di tale repository a modelli standard ed a criteri di apertura costituisce un elemento aggiuntivo qualificante.

S3 Presenza di un **ambiente centralizzato per il riconoscimento dell'utente e l'accesso** a tutte le procedure del sistema mediante le stesse credenziali (es. single-sign-on, identitity management, etc.)

S4 Presenza di **un ambiente centralizzato per la definizione delle regole e dei profili di abilitazione** secondo cui le varie categorie di utenti possono accedere al sistema ed eseguirne le diverse funzionalità.

S5 **Registrazione degli accessi e delle attività** degli utenti, in un log a tre possibili livelli di dettaglio:

minimale	registrazione dei soli accessi al sistema
sintetico	registrazione delle funzionalità eseguite
dettagliato	registrazione, nell'ambito delle varie funzionalità, del dettaglio dei dati acceduti e gestiti dall'utente

S6 **Tracciamento delle variazioni** introdotte al valore dei dati, a due possibili livelli di dettaglio:

semplice	mantenimento della data e dell'autore solo dell'ultima variazione effettuata sul dato
completo	mantenimento della storia di tutte le variazioni effettuate sul dato, ognuna corredata della data e dell'autore della variazione stessa

6.4 Indicatori relativi alla prospettiva implementativa

I1 Unicità di identificazione del paziente da parte di tutte le procedure e continuità del processo di gestione di tutte fasi dell'episodio assistenziale (dalla lista di attesa, alla pre-ospedalizzaione, all'eventuale accesso in pronto soccorso, al ricovero, alla dimissione, alla post-ospedalizzazione), identificato mediante uno stesso codice identificativo, anche se mediante procedure diverse in grado comunque di utilizzare gli stessi dati senza passaggi manuali.

I2 **Registrazione nel sistema informativo dei dati clinici** facenti parte della documentazione del paziente gestita dalla struttura (es. anamnesi, diario clinico, prescrizione terapeutica, referti, schede specialistiche, etc.) sono registrati nel sistema informativo.

La tipologia dei dati registrati nel sistema informativo e la diffusione della registrazione all'interno della struttura sono definiti secondo lo schema seguente

	Classi di rilevanza dei dati clinici	Livello di diffusione
A	Alta rilevanza (oltre il 70% del totale dei casi)	
B	Media rilevanza (fino al 70% del totale casi)	
C	Bassa rilevanza (fino al 35% del totale dei casi)	

I3 **Registrazione nel sistema informativo dei dati infermieristici ed assistenziali** facenti parte della documentazione del paziente gestita dalla struttura (es. diario infermieristico, parametri vitali, requisiti assistenziali, consegne, fragilità, etc.) sono registrati nel sistema informativo.

La tipologia dei dati registrati nel sistema informativo e la diffusione di tale registrazione all'interno della struttura sono definiti secondo lo schema seguente

	Classi di rilevanza dei dati assistenziali i	Livello di diffusione
A	Alta rilevanza (oltre il 70% del totale dei casi)	
B	Media rilevanza (fino al 70% del totale casi)	
C	Bassa rilevanza (fino al 35% del totale dei casi)	

I4 **Utilizzo della firma digitale qualificata** per la certificazione dei dati clinici registrati nel sistema informativo, quantificato -per le diverse tipologie di dati- mediante il **livello di diffusione** secondo l'indice definito al § 6.1

		Livello di diffusione
a)	Referti di esami diagnostici	
b)	Altre registrazioni	

I5 Supporto completo e continuo al **processo di gestione della terapia**, in tutte le sue fasi dalla prescrizione alla somministrazione.
Il livello di utilizzo del sistema informativo nella gestione del processo operatorio è specificato mediante **l'indice di diffusione** secondo i criteri indicati al § 6.1.

I6 Supporto completo e continuo del **processo operatorio** -almeno per le attività extra-operatorie- in tutte le sue fasi dalla programmazione iniziale, alla pianificazione e rendicontazione delle risorse necessarie (inclusi gli impiantabili), fino alla refertazione.
Il livello di utilizzo del sistema informativo nella gestione del processo operatorio è specificato mediante **l'indice di diffusione** secondo i criteri indicati al § 6.1.

I7 Supporto completo e continuo al processo di erogazione degli **esami di laboratorio e di radiodiagnostica** in tutte le fasi: dalla richiesta, alla pianificazione, alla esecuzione e refertazione; permettendo al richiedente la visibilità sullo stato della programmazione e la ricezione del referto come documento informatico.

Il livello di utilizzo del sistema informativo nella gestione del processo operatorio è specificato mediante **l'indice di diffusione** secondo i criteri indicati al § 6.1.

I8 Supporto completo e continuo al **processo di erogazione delle altre prestazioni** (esami diagnostici, consulenze, …), in tutte le fasi: dalla richiesta, alla pianificazione, alla esecuzione e refertazione; permettendo al richiedente la visibilità sullo stato della programmazione e la ricezione del referto come documento informatico.

Le prestazioni sono aggregate secondo le classi di rilevanza specificate al § 6.1, ed indicando per ogni classe il livello di diffusione.

	Classi di rilevanza delle prestazioni	Livello di diffusione
A	Alta rilevanza (oltre il 70% del totale dei casi)	
B	Media rilevanza (fino al 70% del totale casi)	
C	Bassa rilevanza (fino al 35% del totale dei casi)	

I9 **Integrazione dei dati** registrati nelle strutture di archiviazione comuni (clinical repository, enterprise imaging, etc.) secondo un livello di diffusione e di rilevanza come schematizzato nella seguente tabella

	Classi di rilevanza dei dati clinici	Livello di diffusione
A	Alta rilevanza (oltre il 70% del totale dei casi)	
B	Media rilevanza (fino al 70% del totale casi)	
C	Bassa rilevanza (fino al 35% del totale dei casi)	

I10 Utilizzo da parte delle procedure costituenti il sistema informativo del **sistema centralizzato di identificazione utente e abilitazione all'accesso**, dettagliato in termini di un **livello di diffusione** secondo l'indice definito al § 6.1

I11 Utilizzo da parte delle procedure costituenti il sistema informativo del **sistema centralizzato di definizione delle regole e dei profili di abilitazione** delle varie categorie di utenti alle singole funzionalità, dettagliato in termini di un **livello di diffusione** secondo l'indice definito al § 6.1

I12 Possibilità di **consultazione delle informazioni anche mediante dispositivi mobili** (tablet, smartphone), in modo aumentarne l'accessibilità quando e dove necessario, secondo un livello di diffusione come indicato nella seguente tabella

	Classi di rilevanza dei dati clinici	Livello di diffusione
A	Alta rilevanza (oltre il 70% del totale dei casi)	
B	Media rilevanza (fino al 70% del totale casi)	
C	Bassa rilevanza (fino al 35% del totale dei casi)	

I13 Possibilità di **esecuzione delle attività mediante dispositivi mobili** (tablet, smartphone), in modo da evitare la necessità di registrazioni cartacee e successive trascrizioni manuali, secondo un livello di diffusione come indicato nella seguente tabella

	Classi di rilevanza dei dati clinici	Livello di diffusione
A	Alta rilevanza (oltre il 70% del totale dei casi)	
B	Media rilevanza (fino al 70% del totale casi)	
C	Bassa rilevanza (fino al 35% del totale dei casi)	

I14 Presenza di funzionalità in grado di facilitare la **collaborazione e la comunicazione informale** fra operatori -essenzialmente medici ed infermieri- anche relativamente a informazioni non destinate a far parte della documentazione clinica con validità legale, secondo un **indice di diffusione** come definito al § 6.1

I15 Presenza di **funzionalità proattive**, ovvero in grado di evidenziare automaticamente agli utenti situazioni di possibile rilevanza e/o di allarme sulla base dei dati presenti nel sistema.
L'indicatore è dettagliato mediante indice numerico crescente, che assegna un punto ad ogni situazione evidenziata automaticamente dal sistema.
A puro titolo di esempio, si evidenziano i seguenti casi, ampiamente diffusi nelle raccomandazioni e best-practices:

- Evidenziazione di situazioni di potenziale infezione ospedaliera
- Allarme a fronte di valori critici nei risultati di esami di laboratorio ([14])
- Allarme a fronte di valori critici nei parametri vitali
- Verifica di incompatibilità relativamente alla terapia
- Evidenziazione di fattori di rischio e/o fragilità
- Evidenziazione resistenze ad antibiotici

[14] cfr Joint Commission http://www.macoalition.org/Initiatives/docs/CTRgriswold.pdf

I16 Presenza di meccanismi di **riconoscimento automatico e sicuro dell'individuo** (es. RFID, braccialetti con codice a barre, etc.) al momento dell'esecuzione di attività potenzialmente rischiose per il paziente,
L'indicatore è dettagliato mediante indice numerico crescente, che assegna un punto ad ogni processo in cui viene adottato il meccanismo di riconoscimento automatico.
A puro titolo di esempio, si evidenziano i seguenti casi, ampiamente diffusi nelle raccomandazioni e best-practices:

- trasfusioni
- check-in operatorio
- somministrazione della terapia
- trattamenti chemioterapici
- prelievo di campioni
- situazioni anomale o di emergenza (es. Pronto soccorso)

I17 Presenza di una infrastruttura in grado di assicurare la **continuità operativa** -sotto i profili tecnologico, informativo e funzionale- anche in caso di malfunzionamenti parziali del sistema nell'ambito de:

a) i soli settori e processi critici
b) tutti i processi assistenziali

I18 Presenza di una infrastruttura dotata anche di una configurazione di "**disaster recovery**"

6.5 Correlazione fra le caratteristiche del sistema e gli aspetti di sicurezza

Nell'ottica di considerare il sistema informativo come uno strumento aziendale, omogeneo ed integrato, di supporto a tutte le attività della struttura e fortemente radicato nel tessuto organizzativo ed operativo, tutte le caratteristiche del sistema evidenziate dagli indicatori descritti in precedenza contribuiscono alla sicurezza dei processi.

In questo quadro complessivo, tuttavia, le singole caratteristiche del sistema possono contribuire in misura diversa alla riduzione delle diverse tipologie di rischio e possono quindi essere oggetto di specifiche iniziative evolutive e di miglioramento.

La seguente tabella evidenzia con riquadri verdi le correlazioni di maggiore rilevanza fra le caratteristiche del sistema e le singole categorie di rischio, quanto più è intenso il colore tanto più un miglioramento della caratteristica può contribuire alla riduzione del rischio relativo.

Va inoltre considerato come, stante la diversità delle esigenze cliniche ed organizzative legate alle specificità dei vari settori, molto difficilmente il sistema informativo si evolve in modo viene utilizzato in modo contemporaneo ed uniforme in tutta la struttura. A questo proposito sono evidenziate in giallo quelle caratteristiche del sistema in cui l'indice di diffusione è qualificante ai fini della riduzione complessiva dei rischi associati.

Aspetti di sicurezza			livello complessivo della sicurezza	Rischi per la sicurezza del paziente								Rischi dal punto di vista etico e legale					Rispondenza alle normative in generale	Rischi dal punto di vista economico					
		Caratteristiche del sistema		Riconoscimento sicuro	Correttezza della terapia	Errore/incompletezza comunicazione fra sanitari	Dimenticanza	Non considerazione di informazioni rilevanti	Non disponibilità di informazioni rilevanti	Errore nell'inserimento manuale dei dati	Tempestività di reazione a fronte di situazioni di	Controllo nell'accesso alle informazioni	Identificabilità dell'autore di una operazione	Identificabilità del valore di un dato ad una certa data	Perdita di informazioni	Dolo		Aumento dei tempi di degenza	Ripetizione inutile di esami/attività	Non appropriatezza di esami/attività	Tempi e risorse necessari per eseguire una attività	Canoni di assicurazione e risarcimenti
O - Prospettiva organizzativa																							
	O1	Presenza di una funzione aziendale preposta alla sicurezza nel SI	x																				
	O2	Collaborazione con le funzioni preposte al rischio clinico	x	x	x	x	x	x	x	x	x												
	O3	Pianificazione periodica complessiva delle iniziative inerenti la sicurezza	x																				
	O4	Assessment periodico dello stato di sicurezza complessivo	x																				
	O5	Monitoraggio e registrazione degli incidenti inerenti la sicurezza	x																				
	O6	Gestione di un "libro bianco" dei possibili miglioramenti	x																				
	O7	Esistenza di una funzione aziendale preposta al rilascio delle credenziali di accesso										x				x	x						
	O8	Esistenza di una funzione aziendale preposta alla definizione dei profili di abilitazione										x				x	x						
	O9	Utilizzo di vocabolari e codifiche uniformi per l'indentificazione di dati e processi				x		x	x						x								
	O10	Presenza di criteri per la regolamentazione dell'uso di dispositivi personali									x	x				x	x					x	

Aspetti di sicurezza			livello complessivo della sicurezza	Rischi per la sicurezza del paziente									Rischi dal punto di vista etico e legale						Rischi dal punto di vista economico						
				Riconoscimento sicuro	Correttezza della terapia	Errore/incompletezza comunicazione fra sanitari	Dimenticanza	Non considerazione di informazioni rilevanti	Non disponibilità di informazioni rilevanti	Errore nell'inserimento manuale dei dati	Tempestività di reazione a fronte di situazioni di	Controllo nell'accesso alle informazioni	Identificabilità dell'autore di una operazione	Identificabilità del valore di un dato ad una certa data	Perdita di informazioni	Dolo	Rispondenza alle normative in generale	Aumento dei tempi di degenza	Ripetizione inutile di esami/attività	Non appropriatezza di esami/attività	Tempi e risorse necessari per eseguire una attività	Canoni di assicurazione e risarcimenti	
Caratteristiche del sistema																									
S - Prospettiva strutturale																									
	S1	Presenza di un repository centralizzato per l'integrazione di tutte le informazioni cliniche, assistenziali ed operative						x	x																
	S2	Presenza di un archivio aziendale per l'integrazione di tutte le immagini e dati multimediali						x	x																
	S3	Presenza di un ambiente centralizzato per il riconoscimento dell'utente e l'accesso al sistema										x	x				x								
	S4	Esistenza di un ambiente centralizzato per la definizione dei profili di abilitazione										x					x								
	S5	Registrazione in un log di tutte le attività degli utenti											x				x								
	S6	Mantenimento della storia di tutte le variazioni ai singoli dati											x	x	x										

Aspetti di sicurezza			livello complessivo della sicurezza	Rischi per la sicurezza del paziente									Rischi dal punto di vista etico e legale						Rischi dal punto di vista economico						
				Riconoscimento sicuro	Correttezza della terapia	Errore/incompletezza comunicazione fra sanitari	Dimenticanza	Non considerazione di informazioni rilevanti	Non disponibilità di informazioni rilevanti	Errore nell'inserimento manuale dei dati	Tempestività di reazione a fronte di situazioni di	Controllo nell'accesso alle informazioni	Identificabilità dell'autore di una operazione	Identificabilità del valore di un dato ad una certa data	Perdita di informazioni	Dolo	Rispondenza alle normative in generale	Aumento dei tempi di degenza	Ripetizione inutile di esami/attività	Non appropriatezza di esami/attività	Tempi e risorse necessari per eseguire una attività	Canoni di assicurazione e risarcimenti	
Caratteristiche del sistema																									
I- Prospettiva implementativa																									
	I1	Continuità del processo di gestione paziente all'interno dell'episodio assistenziale		x	x	x	x	x	x			x	x+					x	x	x	x				
	I2	Registrazione dei dati clinici			x	x		x	x				x	x	x					x					
	I3	Registrazione dei dati assistenziali				x		x	x				x	x	x					x					
	I4	Utilizzo della firma digitale						x	x				x+				x					x			
	I5	Continuità del processo di gestione delle terapie, dalla prescrizione alla somministrazione			x								x												
	I6	Continuità del processo operatorio						x	x	x			x				x	x				x			
	I7-I8	Continuità nella richiesta, programmazione, esecuzione e refertazione di esami e consulenze				x		x	x	x			x					x	x			x			
	I9	Integrazione dei dati registrati nei repository centrali				x+		x+	x+	x+		x+	x+								x+				
	I10	Utilizzo di meccanismi centralizzati di riconoscimento utente e accesso al sistema										x+													
	I11	Utilizzo di meccanismi centralizzati per regole e profili di abilitazione										x+	x+												
	I12	Accesso in mobilità per sola consultazione				x	x	x	x		x														
	I13	Accesso in mobilità per operatività complete				x	x	x	x	x+	x							x				x			
	I14	Supporto alle comunicazioni ed allo scambio di informazioni fra operatori				x	x																		
	I15	Esistenza di meccanismi proattivi di allarme automatico					x	x			x													x	
	I16	Esistenza di meccanismi per il riconoscimento del paziente		x	x															x	x				
	I17	Garanzia di continuità dell'infrastruttura																							
	a)	business continuity nelle sole aree critiche	x																						
	b)	business continuity in tutti i processi assistenziali	x+																						
	I18	Infrastruttura di disaster recovery	x++													x									

Impatto crescente in funzione della quantità e della diffusione nell'azienda

7. Modello per la classificazione in livelli della sicurezza nei sistemi informativi

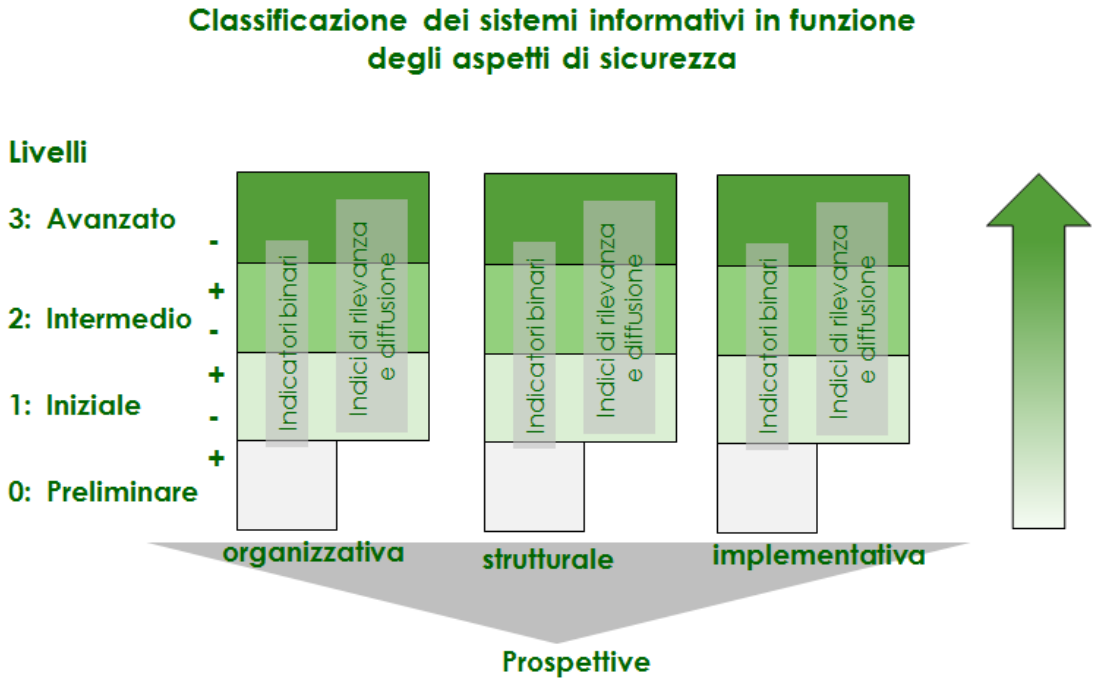
7.1 Livelli di classificazione

Sulla base di quanto emerso dallo studio, sia in termini di caratteristiche dei sistemi che di scenari implementati nelle diverse aziende, in questa sezione viene proposta una classificazione in livelli della maturità dei sistemi informativi dal punto di vista della loro sicurezza.

Traendo spunto dall'approccio adottato nell' HiMMS "EMR Adoption Model", al fine di essere facilmente individuabile, ogni livello descrive uno scenario operativo, mediante indicatori basati sulla presenza o meno di caratteristiche facilmente riscontrabili in base alla gestione ed all'utilizzo corrente del sistema nell'organizzazione.

Secondo l'approccio multi-dimensionale di analisi adottato, anche i livelli si articolano secondo tre prospettive: quella organizzativa, quella strutturale e quella implementativa.

Per ogni prospettiva sono definiti quattro livelli, secondo una scala crescente di maturità e completezza dal valore **0** al valore **3**, in cui **0** indica uno stato iniziale e **3** lo scenario più avanzato e, di conseguenza, più maturo in termini di sicurezza nella sua accezione completa.



Molto sinteticamente, gli scenari corrispondenti ad i singoli livelli possono essere descritti come segue

Livello 0 – Preliminare

Denota un contesto in cui le problematiche inerenti la sicurezza sono ancora affrontate quasi esclusivamente dal punto di vista tecnologico, secondo criteri e soluzioni frammentate senza una visione integrata nell'azienda.

Livello 1 – Iniziale

Denota un contesto in cui l'azienda dimostra sensibilità e di aver cominciato ad affrontare in modo organico le problematiche inerenti la sicurezza.
Le conseguenti caratteristiche strutturali ed operative del sistema informativo sono però ancora ancora ad uno stato iniziale, circoscritte ad un numero limitato di settori e di processi.

Livello 2 – Intermedio

Denota un contesto in cui l'azienda dimostra di affrontare in modo organico le problematiche inerenti la sicurezza.
Sono presenti nel sistema informativo caratteristiche strutturali in grado di contribuire alla sicurezza dei dati e dei processi anche mediante la centralizzazione di informazioni, regole e funzionalità.
Le operatività sono tuttavia ancora non ampiamente e non uniformemente diffuse in tutta la struttura.

Livello 3 – Avanzato

Denota un contesto in cui l'azienda affrontare in modo organico le problematiche inerenti la sicurezza, tenendo in forte considerazione anche le problematiche relative al rischio clinico ed operando secondo un approccio propositivo e di continuo miglioramento.
Sono presenti nel sistema informativo caratteristiche strutturali in grado di contribuire alla sicurezza dei dati e dei processi anche mediante la centralizzazione di informazioni, regole e funzionalità.
Le operatività sono ampiamente ed uniformemente diffuse in tutta la struttura.
Sono inoltre presenti meccanismi proattivi per l'evidenziazione automatica di situazioni di rilevanza e la prevenzione del rischio.

7.2 Scenari caratterizzanti i singoli livelli

Lo scenario complessivo caratterizzante ogni livello è brevemente descritto nel seguito. Nei paragrafi successivi sono formalizzati i singoli indicatori da valutare per la classificazione.

7.2.1 Livello 0: "Preliminare"

Denota un contesto in cui le problematiche inerenti la sicurezza sono ancora affrontate quasi esclusivamente dal punto di vista tecnologico, secondo criteri e soluzioni frammentate al di fuori di una visione integrata nell'azienda.

Dal punto di vista organizzativo

- manca una funzione aziendale preposta alla sicurezza nel sistema informativo, di conseguenza mancano anche momenti di pianificazione e di verifica
- la definizione e la gestione dei criteri di abilitazione è demandata ai singoli settori

Dal punto di vista strutturale

- il sistema si presenta frammentato in aree funzionali ed informative separate e non è presente un repository in cui poter integrare i dati operativi e sanitari rendendoli disponibili a tutti i settori
- le immagini e i dati multimediali sono registrati solo localmente in alcuni settori, senza la possibilità di integrazione e correlazione con altri dati clinici del paziente
- manca un meccanismo centralizzato in grado di controllare e registrare in modo uniforme gli accessi al sistema

Dal punto di vista implementativo

L'operatività rispecchia la frammentazione complessiva del sistema, ed i processi operano separatamente nei vari settori, in particolare:

- non è garantita ovunque la continuità ed uniformità del processo di gestione dell'episodio assistenziale (identificazione univoca dalla lista di attesa, alla pre-ospedalizzazione, al ricovero e dimissione)
- vengono registrati nel sistema solo alcuni dati clinici di maggiore rilevanza, ma con un livello di diffusione molto basso nella struttura e solo in settori e procedure separate
- con l'unica eccezione -parziale- degli esami di laboratorio e di radiodiagnostica, non sono supportati con continuità i processi intersettoriali di richiesta, programmazione, esecuzione e refertazione delle prestazioni, che operano separatamente nei vari settori, che interagendo anche tramite supporti cartacei e senza poter attingere ad un patrimonio di informazioni comuni e rilevanti.

7.2.2 Livello 1: "Iniziale"

Denota un contesto in cui l'azienda dimostra sensibilità e di aver cominciato ad affrontare in modo organico le problematiche inerenti la sicurezza. Le conseguenti caratteristiche strutturali ed operative del sistema informativo sono però ancora ancora ad uno stato iniziale, circoscritte ad un numero limitato di settori e di processi.

Dal punto di vista organizzativo

- è presente una funzione aziendale preposta alla sicurezza nel sistema informativo, che ha definito -o sta definendo- un piano organico per tutti gli aspetti inerenti la sicurezza
- sono presenti funzioni di monitoraggio per la verifica del regolare funzionamento e la registrazione di eventuali incidenti
- la definizione e la gestione dei criteri di abilitazione per i singoli utenti è centralizzata (nota: questo si riferisce solo alla esistenza di una funzione aziendale preposta, non si traduce necessariamente nella presenza di un meccanismo unificato di controllo degli accessi)

Dal punto di vista strutturale

- l'architettura del sistema comprende un archivio centrale (es. Clinical Repository) potenzialmente in grado di registrare ed integrare i dati operativi e sanitari rendendoli disponibili a tutti i settori
- le immagini e i dati multimediali sono però ancora registrati solo localmente in alcuni settori, senza la possibilità di integrazione e correlazione con altri dati clinici del paziente
- è presente (anche se non utilizzato necessariamente da tutte le applicazioni) un meccanismo unificato di controllo degli accessi (es. single-sign-on)

Dal punto di vista implementativo

L'operatività rispecchia la frammentazione complessiva del sistema, ed i processi operano separatamente nei vari settori, in particolare:

- è garantita ovunque la continuità ed uniformità del processo di gestione dell'episodio assistenziale (identificazione univoca dalla lista di attesa, alla pre-ospedalizzazione, al ricovero e dimissione);
- vengono registrati nel sistema solo dati clinici di maggiore rilevanza, ma con un livello di diffusione basso e senza una effettiva integrazione nel Repository, in grado di rendere le informazioni fruibili anche agli altri settori della struttura.
- i processi di richiesta, programmazione, esecuzione e refertazione degli esami di laboratorio e di radiodiagnostica, sono supportati con continuità in tutta la struttura, mentre non solo sono (o lo sono a livello di diffusione estremamente basso) gli altri processi intersettoriali che quindi continuano ad interagire anche tramite supporti cartacei e senza poter attingere ad un patrimonio di informazioni comuni e rilevanti.

7.2.3 Livello 2: "Intermedio"

Denota un contesto in cui l'azienda dimostra di affrontare in modo organico le problematiche inerenti la sicurezza.
Sono presenti nel sistema informativo caratteristiche strutturali in grado di contribuire alla sicurezza dei dati e dei processi anche mediante la centralizzazione di informazioni, regole e funzionalità.
Le operatività sono tuttavia ancora non ampiamente e non uniformemente diffuse in tutta la struttura.

Dal punto di vista organizzativo

- La funzione aziendale preposta alla sicurezza nel sistema informativo opera sulla base di un piano organico per tutti gli aspetti inerenti la sicurezza, che vengono monitorizzati individualmente e verificati nella loro complesso mediante periodici momenti di assessment;
- la definizione e la gestione dei criteri di abilitazione per i singoli utenti è centralizzata.
- sono definiti ed adottati vocabolari e codifiche comuni in tutta la struttura, almeno per quelle tipologie di informazioni di notevole rilevanza nel contesto specifico.

Dal punto di vista strutturale

- l'architettura del sistema è in grado di integrare sia i dati strutturati che quelli multimediali in strutture centralizzate (es. Clinical Data Repository ed Enterprise Imaging) rendendoli disponibili a tutti i settori, secondo meccanismi e regole gestibili centralmente, in modo da garantire l'implementazione rapida e la diffusione uniforme in tutta la struttura delle normative e delle regole aziendali;
- è presente un meccanismo unificato di controllo degli accessi (es. single-sign-on) e viene mantenuto un log degli accessi al sistema da parte dei singoli utenti

Dal punto di vista implementativo

L'operatività rispecchia la frammentazione complessiva del sistema, ed i processi operano separatamente nei vari settori, in particolare:

- è garantita ovunque la continuità ed uniformità del processo di gestione dell'episodio assistenziale (identificazione univoca dalla lista di attesa, alla pre-ospedalizzazione, al ricovero e dimissione);
- la registrazione nel sistema dati clinici ed assistenziali di maggiore rilevanza è ampiamente diffusa nei vari settori dell'azienda, ed i dati registrati, anche autenticati con firma digitale, sono integrati nel repository centrale e sono acceduti anche da altri settori;
- i processi di richiesta, programmazione, esecuzione e refertazione di prestazioni sono supportati con continuità, senza bisogno di trascrizioni cartacee, struttura almeno per l'esecuzione delle attività di maggiore rilevanza
- l'infrastruttura tecnologica assicura la continuità operativa almeno per i processi più critici e consente l'accesso in mobilità per la consultazione delle informazioni di maggiore rilevanza nello specifico contesto.

7.2.4 Livello 3: "Avanzato"

Denota un contesto in cui l'azienda affrontare in modo organico le problematiche inerenti la sicurezza, tenendo in forte considerazione anche le problematiche relative al rischio clinico ed operando secondo un approccio propositivo e di continuo miglioramento.
Sono presenti nel sistema informativo caratteristiche strutturali in grado di contribuire alla sicurezza dei dati e dei processi anche mediante la centralizzazione di informazioni, regole e funzionalità.
Le operatività sono ampiamente ed uniformemente diffuse in tutta la struttura.
Sono inoltre presenti meccanismi proattivi per l'evidenziazione automatica di situazioni di rilevanza e la prevenzione del rischio.

Dal punto di vista organizzativo

- La funzione aziendale preposta alla sicurezza nel sistema informativo opera in collaborazione con la funzione responsabile del rischio clinico, sulla base di un piano organico e con momenti periodi di assessment complessivo.
- Il funzionamenti del sistema viene regolarmente monitorizzato, gestendo anche un "libro bianco" di possibili miglioramenti
- E' centralizzata sia la definizione delle abilitazioni all'accesso individuale che l'assegnazione delle regole di abilitazione alle singole funzionalità per le varie tipologie di utenza.
- sono ampiamente definiti ed adottati vocabolari e codifiche comuni in tutta la struttura.

Dal punto di vista strutturale

- l'architettura del sistema è in grado di integrare sia i dati strutturati che quelli multimediali in strutture centralizzate (es. Clinical Data Repository ed Enterprise Imaging) rendendoli disponibili a tutti i settori, anche a livello secondo meccanismi e regole di abilitazione gestibili centralmente;
- è presente un meccanismo unificato per l'identificazione dell'utente ed il controllo degli accessi, utilizzato in modo pressoché totale in tutto il sistema;
- Viene mantenuto un log degli delle attività dei singoli utenti nonché la storia di tutte le variazioni apportate nel tempo ai singoli dati.

Dal punto di vista implementativo

- è garantita ovunque la continuità ed uniformità del processo di gestione dell'episodio assistenziale (identificazione univoca dalla lista di attesa, alla pre-ospedalizzazione, al ricovero e dimissione);
- la registrazione nel sistema dati clinici ed assistenziali è ampiamente diffusa nei vari settori dell'azienda anche per i dati di minore rilevanza, ed i dati registrati, anche autenticati con firma digitale, sono integrati nel repository centrale e sono acceduti anche da altri settori;
- i processi di richiesta, programmazione, esecuzione e refertazione di prestazioni sono supportati con continuità, senza bisogno di trascrizioni cartacee, nella maggior parte della struttura, anche per le prestazioni di minore rilevanza

- sono presenti funzionalità proattive, in grado di evidenziare autonomamente situazioni di allarme e di potenziale rischio e meccanismi di riconoscimento sicuro dell'individuo in processi critici.
- l'infrastruttura tecnologica assicura la continuità operativa per tutti i processi assistenziali anche con una configurazione di "disaster recovery" e consente l'accesso in mobilità non solo per la consultazione delle informazioni ma anche per la effettuazione di transazioni complesse.

7.3 Check-list di valutazione dei livelli secondo gli indicatori

Legenda

Indice di rilevanza		% rispetto al totale dei casi (pazienti)
A	Alto	oltre 70%
B	Medio	fino a 70%
C	Basso	fino a 30%

Indice di diffusione		% rispetto al totale degli elementi di rilevanza
A+	Molto alto	superiore ad 85%
A	Alto	fino a 85%
B	Medio	fino a 65%
C	Basso	fino a 35%
C-	Molto basso	inferiore a 10%

Prospettiva organizzativa					Livello			
					0	1	2	3
O1	Presenza di una funzione aziendale responsabile della sicurezza del SI nel suo complesso, secondo i diversi profili di rischio		SI/NO		NO	SI	SI	SI
O2	Collaborazione fra la funzione sicurezza e la funzione rischio clinico		SI/NO					SI
O3	Gestione di un piano organico per tutti gli aspetti inerenti la sicurezza		SI/NO		NO	SI	SI	SI
O4	Presenza di momenti di assessment periodico		SI/NO		NO		SI	SI
		frequenza						1 / anno
O5	Monitoraggio del sistema e registrazone incidenti		SI/NO			SI	SI	SI
O6	Gestione di un libro bianco dei miglioramenti		SI/NO					SI
O7	Definizione centralizzata delle credenziali di accesso		SI/NO			SI	SI	SI
O8	Definizione centralizzata dei profili di abilitazione		SI/NO					SI
O9	Utilizzo di vocabolari e codifiche uniformi		SI/NO				SI	SI
		Informazioni di Alta rilevanza	indice di diffusione				*medio*	*alto*
		Informazioni di Media rilevanza	indice di diffusione					*alto*
		Informazioni di Bassa rilevanza	indice di diffusione					*basso*
O10	Presenza di regole per l'utilizzo di dispositivi mobili e personali da parte di operatori sanitari e di pazienti							

Prospettiva strutturale					Livello			
					0	1	2	3
S1	Presenza di un repository per l'integrazione di tutti i dati clinici, assistenziali, operativi (es. Clinical Data Repository)		SI/NO		NO	SI	SI	SI
S2	Presenza di un repository per l'integrazione di tutte le immagini e dati multimediali (es. Enterprise Imaging)		SI/NO		NO		SI	SI
S3	Presenza di un meccanismo centralizzato di identificazione utente e abilitazione accesso (es. single-sign-on)		SI/NO		NO	SI	SI	SI
S4	Presenza di ambiente centralizzato di gestione delle regole e dei profili di abilitazione		SI/NO				SI	SI
S5	Gestione di un log di accesso e di attività	minimale	SI/NO			SI	SI	SI
		sintetico	SI/NO				SI	SI
		dettagliato	SI/NO					SI
S6	Registrazione della storia delle variazioni ai dati	sintetico	SI/NO				SI	SI
		completo						SI

Prospettiva implementativa					Livello			
					0	1	2	3
I1	Unicità di identificazione paziente e continuità dell'episodio assistenziale in tutte le fasi		SI/NO			SI	SI	SI
I2	Registrazione dei dati clinici	Dati di Alta rilevanza	indice di diffusione		molto basso	basso	medio	alto
		Dati di Media rilevanza	indice di diffusione			molto basso	basso	medio
		Dati di Bassa rilevanza	indice di diffusione					
I3	Registrazione dei dati assistenziali	Dati di Alta rilevanza	indice di diffusione				basso	alto
		Dati di Media rilevanza	indice di diffusione				molto basso	medio
		Dati di Bassa rilevanza	indice di diffusione					
I4	Utilizzo della firma digitale		SI/NO				SI	SI
		Diffusione					basso	medio
I5	Conitnuità del percorso di gestione della terapia		SI/NO				SI	SI
		Diffusione						medio
I6	Continuità del processo (extra-) operatorio		SI/NO				SI	SI
		Diffusione	indice di diffusione				alto	molto alto
I7	Conitnuità del processo di richiesta ed esecuzione di prestazioni di laboratorio e radiodiagnostica		SI/NO			SI	SI	SI
		Diffusione	indice di diffusione			alto	molto alto	molto alto
I8	Continuità del processso di richiesta ed esecuzione di altre prestazioni		SI/NO				SI	SI
		Prestazioni di Alta rilevanza	indice di diffusione				alto	molto alto
		Prestazioni di Media rilevanza	indice di diffusione				medio	alto
		Prestazioni di Bassa rilevanza	indice di diffusione					medio
I9	Integrazione dei dati e delle immagini nei repository centrali						SI	SI
		Dati di Alta rilevanza	indice di diffusione				alto	molto alto
		Dati di Media rilevanza	indice di diffusione				medio	alto
		dati di Bassa rilevanza	indice di diffusione					medio
I10	Utilizzo di funzioni centralizzate di identificazione utente ed abilitazione all'accesso		SI/NO				SI	SI
		Diffusione	indice di diffusione				basso	medio
I11	Utilizzo del sistema centralizzato delle regole e dei profili di abilitazione		SI/NO					SI
		Diffusione	indice di diffusione					medio
I12	Consultazione dati clinici in mobilità		SI/NO				SI	SI
		Dati di Alta rilevanza	indice di diffusione				medio	alto
		Dati di Media rilevanza	indice di diffusione					medio
		Dati di Bassa rilevanza	indice di diffusione					
I13	Esecuzione attività in mobilità		SI/NO				SI	SI
		Attività di Alta rilevanza	indice di diffusione				medio	alto
		Attività di Media rilevanza	indice di diffusione					medio
		Attività di Bassa rilevanza	indice di diffusione					
I14	Presenza di meccanismi di comunicazione informale fra operatori		SI/NO					SI
		Diffusione	numero processi					
I15	Presenza di meccansimi proattivi (allarmi e correlazioni automatiche)		SI/NO					SI
		Diffusione	numero processi					
I16	Presenza di meccanismi di riconoscimento automatico del paziente		SI/NO					SI
		Diffusione	numero processi					
I17	Configurazione di business-continuity	processi critici	SI/NO		NO		SI	SI
		tutti i processi assistenziali	SI/NO					SI
I18	Configurazione di disaster recovery		SI/NO					SI

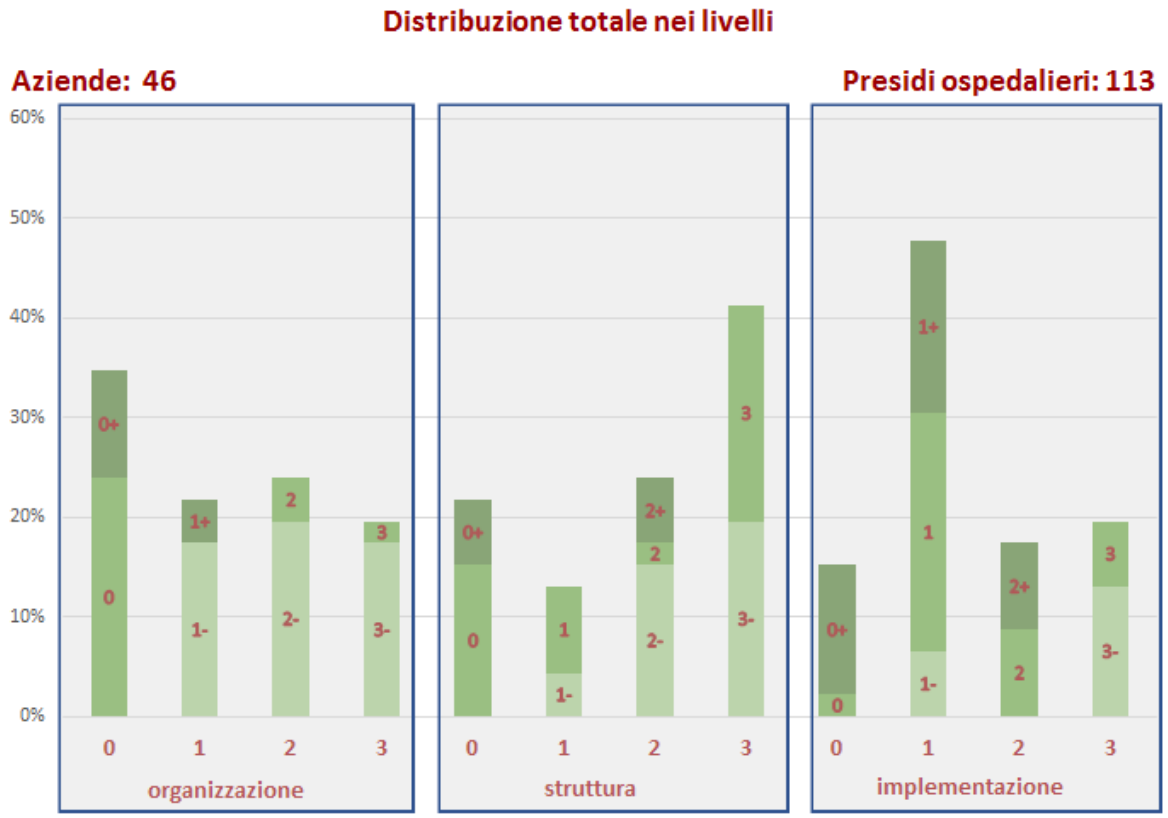
8. Posizionamento delle aziende partecipanti secondo il modello di classificazione

Nei seguenti prospetti è indicata la distribuzione statistica dei sistemi sanitari studiati nell'ambito dei vari livelli di classificazione proposti.

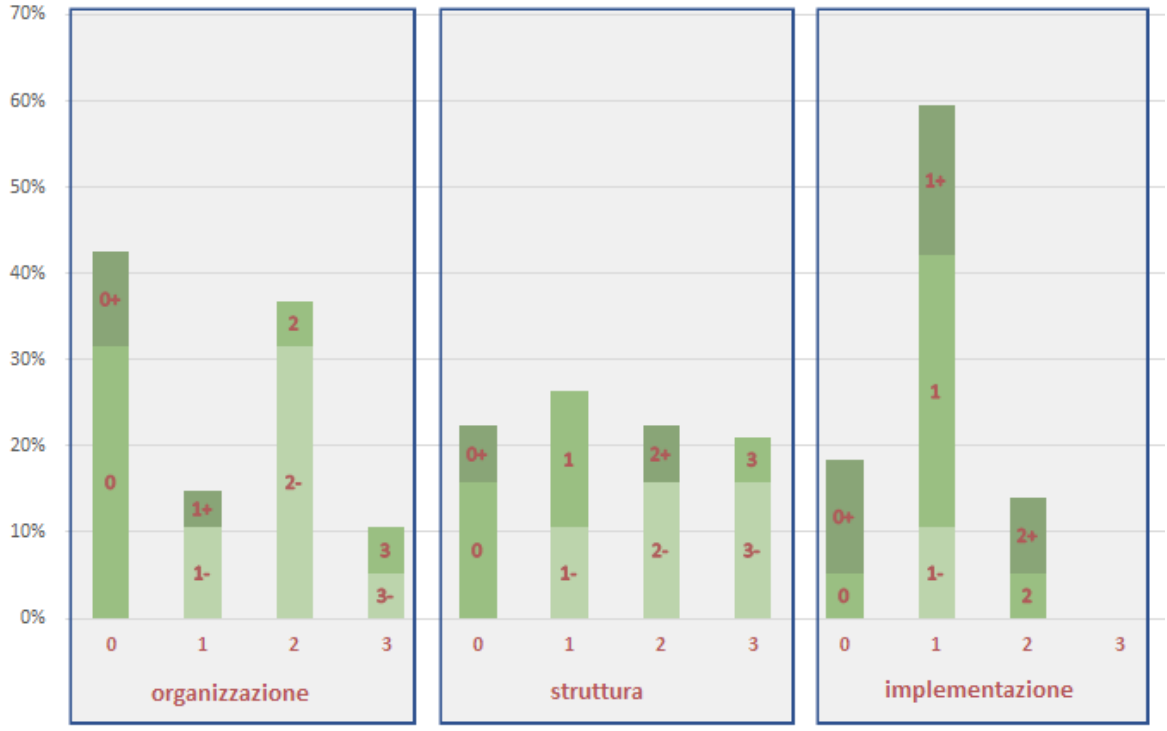
Come evidenziato in precedenza, la definizione di una metodologia uniforme di analisi e di classificazione costituiva un obiettivo dello studio. Di conseguenza, gli argomenti oggetto del questionario compilato dalle aziende partecipanti non hanno una corrispondenza speculare con gli indicatori finali, formalizzati nella metodologia (indicatori che sono stati per l'appunto formalizzati anche sulla base dei contributi forniti dalle aziende partecipanti).

L'assegnazione dei "livelli di sicurezza" ai singoli questionari ricevuti, pertanto, non è frutto di un semplice algoritmo deterministico, ma **va intesa a livello qualitativo** in quanto basata anche su passaggi interpretativi di quanto dichiarato dai singoli partecipanti nel questionario.

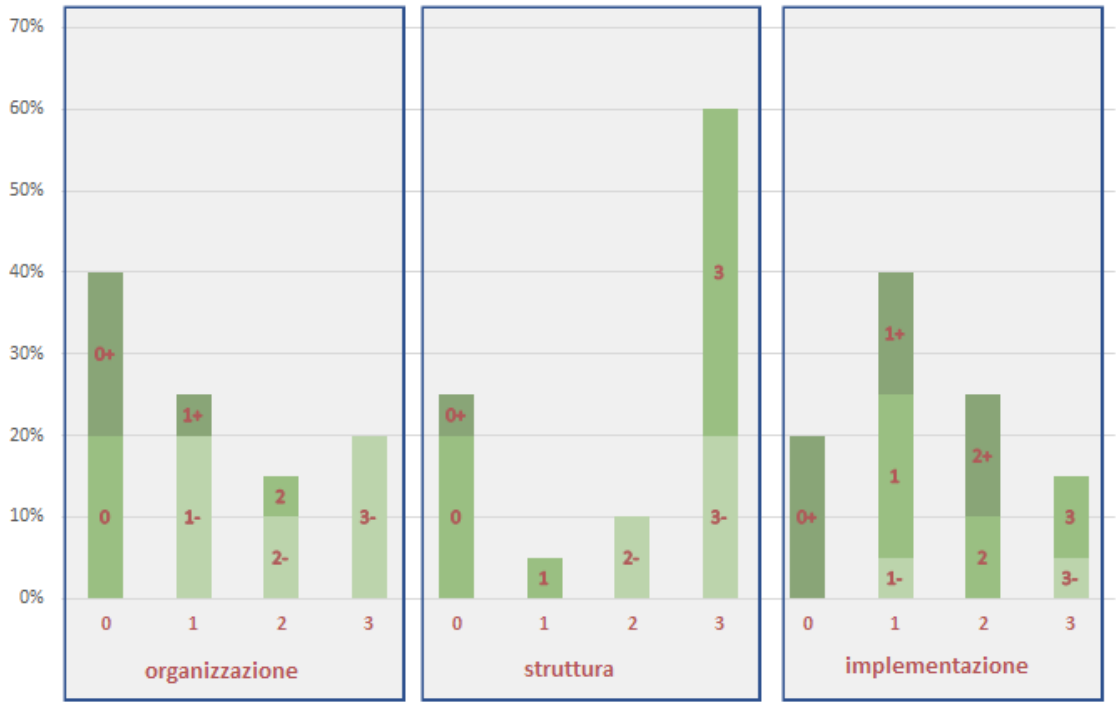
Va inoltre sottolineato che gli indici relativi alla rilevanza ed alla diffusione (non esposti nei seguenti grafici), in quanto non esplicitamente richiesti nei questionari sono stati derivati a livello qualitativo in fase di analisi, sulla base del quadro complessivo che si poteva evincere dai dati forniti.



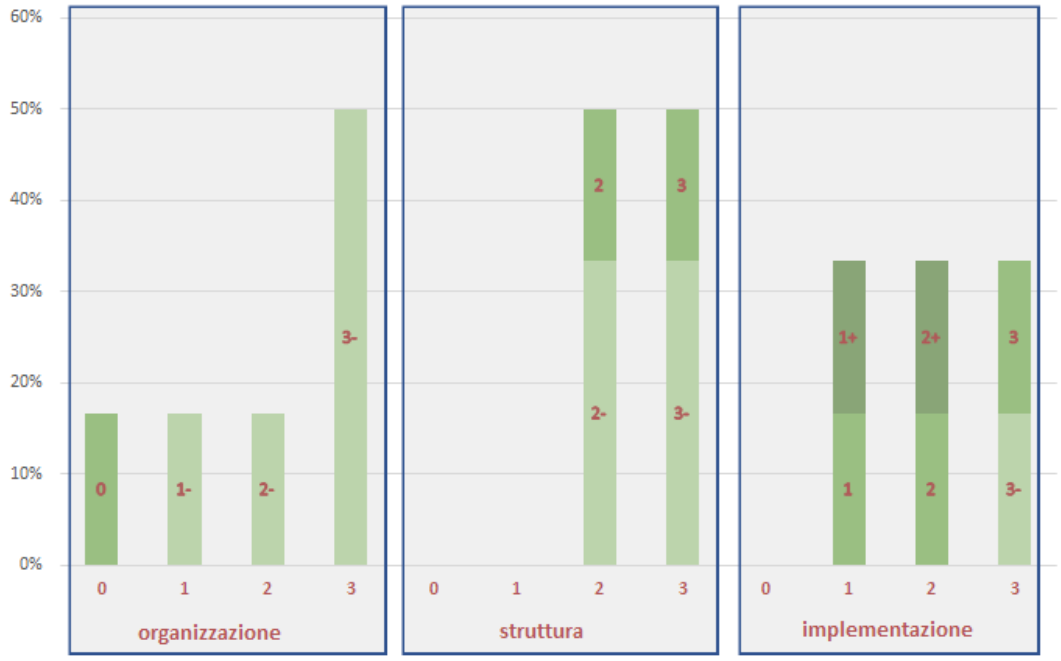
Distribuzione ASL nei livelli



Distribuzione Aziende Ospedaliere e Policlinici Universitari nei livelli



Distribuzione IRCCS nei livelli



9. Bibliografia

Normative

- Normative sulla privacy
  http://www.garanteprivacy.it/web/guest/home/provvedimenti-normativa/normativa
  http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1637608
- Regolamento europeo
  http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-internazionale
- Agenzia per l'Italia Digitale Circolare 17 marzo 2017, n. 1/2017, "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)(17A02399)", (Gazzetta Ufficiale n.79 del 4-4-2017)
- Linee guida in materia di Dossier sanitario - 4 giugno 2015 *(Pubblicato sulla Gazzetta Ufficiale n. 164 del 17 luglio 2015)*
- Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini – Normativa e prassi. Rep. Atti n. 81/CSR del 4 aprile 2012
- Decreto-legge 18 ottobre 2012, n. 179 "Sezione IV Sanità Digitale" (*Gazzetta Ufficiale n. 245 del 19 ottobre 2012*)
- Decreto Ministeriale 26 luglio1993 "Disciplina del flusso informativo sui dimessi dagli Istituti di ricovero pubblici e privati " (*Gazzetta Ufficiale n. 180 del 3 agosto 1993*)
- Ministero della Sanità - Circolare n. 900.2/2.7/190 del 14 Marzo 1996, "Guida alla corretta compilazione e tenuta del registro operatorio"

Standard e linee guida

- ISO/IEC 10746:2009 "Information Technology - Open distributed processing – Reference model"
- ISO/IEC 27001:2013 "Information Security Management"
- ISO 12967:2009 "Health Informatics – Service Architecture"
- ISO 9001:2015 "Quality Management System – Requirements"
- HiMMS Analytics – EMRAM: Electronic Medical Record Adoption Model
  http://www.himssanalytics.org/emram
- UK National Data Guardian "Recommendations to strengthen security of health and care information"
  https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

Rischio clinico e sicurezza

- Joint Commission on Accreditation of Healthcare Organizations
  http://www.jointcommissioninternational.org/
  - 2017 National Patient Safety goals
  - Sentinel Event Policy
  - Critical test result management,
  - Communications during patients hand-over
- Ministero della Salute, "Raccomandazioni agli operatori"
  http://www.salute.gov.it/portale/temi/p2_6.jsp?id=250&area=qualita&menu=sicurezza
- Agenas – Rischio clinico e sicurezza del paziente
  http://www.agenas.it/aree-tematiche/qualita/rischio-clinico-e-sicurezza-del-paziente
- Sicurezza dei pazienti e gestione del rischio clinico: Manuale per la formazione degli operatori sanitari. Corso di formazione del Ministero della Salute; Dipartimento della qualità; Direzione

generale della programmazione sanitaria, dei livelli essenziali di assistenza e dei Principi etici del sistema, in collaborazione con FNOMCeO e IPASVI. Roma, Maggio 2007.

Appropriatezza e organizzazione

- Ministero della salute "Manuale di formazione per il governo clinico: Appropriatezza" http://www.salute.gov.it/imgs/C_17_pubblicazioni_1826_allegato.pdf
- Fontana, "Clinical Governance, una prospettiva clinica e gestionale", Franco Angeli, 2005, https://books.google.it/books?id=-Cjatz8aTSgC&lpg=PA72&ots=VO9aCuhfwS&dq=costo%20errori%20clinici&hl=it&pg=PA4#v=onepage&q=costo%20errori%20clinici&f=false

Ruolo dell'ICT sulla qualità e costi del processo medico

- Ten Commandments for Effective Clinical Decision Support: Making the Practice of Evidence-based Medicine a Reality, https://academic.oup.com/jamia/article/10/6/523/760582/Ten-Commandments-for-Effective-Clinical-Decision
- Restuccia, Hospital implementation of health information technology and quality of care: are they related? http://www.biomedcentral.com/1472-6947/12/109
- Health Information Technology And Patient Safety: Evidence From Panel Data, http://content.healthaffairs.org/content/28/2/357.abstract
- The Effects of Health Information Technology on the Costs and Quality of Medical Care; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4415264/
- Politecnico di Milano, osservatorio ICT in sanità https://www.digital4.biz/executive/approfondimenti/sanita-dal-digitale-un-possibile-risparmio-di-15-miliardi-l-anno_43672151674.htm

Valutazione dei rischi ed impatto sui costi

- AGENAS – Medicina difensiva, Diffusione e impatto economico, http://www.agenas.it/images/agenas/monitor/quaderno/pdf/15_medicina_difensiva.pdf
- Kaplan, Haas "How not to cut Health Care Costs", Harvard Business Review https://hbr.org/2014/11/how-not-to-cut-health-care-costs
- IlSole24ore http://www.sanita24.ilsole24ore.com/pdf2010/Sanita2/_Oggetti_Correlati/Documenti/Regioni-e-Aziende/presentazione_nisan.pdf?uuid=AbexJUuG http://www.sanita24.ilsole24ore.com/art/regioni-e-aziende/2013-05-07/politecnico-milano-lict-miliardi-085503.php?uuid=AbpCjhtH
- Ospedale Sicuro - Costi umani ed economici http://www.ospedalesicuro.eu/storia/tutela/costi.html
- Gestione integrata del rischio clinico e del rischio assicurativo, http://www.giot.it/wp-content/uploads/2015/06/10_Macri_Medicina_Legale1.pdf