ISSN 2420-7888

Ratio Iuris

GOVERNANCE INTEGRATA DELLA SICUREZZA DELLE CURE E DELL'INNOVAZIONE SANITARIA: UN MODELLO GIURIDICO-ORGANIZZATIVO PER LE AZIENDE SANITARIE PUBBLICHE

Integrated Governance of Patient Safety and Healthcare Innovation: A Legal and Organisational Model for Public Healthcare Organisations

Autore: Pierluigi Crusco

Abstract

La trasformazione digitale dei sistemi sanitari, l'espansione della telemedicina, l'impiego crescente di sistemi di intelligenza artificiale e la progressiva interoperabilità dei dati clinici stanno modificando non soltanto le modalità di erogazione delle prestazioni, ma anche le categorie tradizionali attraverso le quali vengono governati il rischio clinico e la responsabilità delle organizzazioni sanitarie.

Nel sistema italiano, la sicurezza delle cure, qualificata dalla legge n. 24/2017 quale parte costitutiva del diritto alla salute, non può più essere circoscritta alla prevenzione dell'errore clinico in senso stretto. La sicurezza contemporanea comprende anche il rischio organizzativo, informativo, tecnologico, algoritmico e cibernetico. Parallelamente, il Regolamento (UE) 2024/1689 sull'intelligenza artificiale (AI Act), il Regolamento (UE) 2025/327 sullo European Health Data Space (EHDS), il Regolamento (UE) 2016/679 e la legislazione italiana sull'intelligenza artificiale stanno progressivamente configurando un sistema multilivello di obblighi destinato a incidere direttamente sulla governance delle aziende sanitarie.

Il contributo propone un modello di **governance integrata della sicurezza delle cure e dell'innovazione sanitaria**, fondato sul superamento della frammentazione tra clinical risk management, governo giuridico, sanità digitale, gestione dei dati, cybersecurity e valutazione delle tecnologie innovative. Il modello prevede una funzione permanente di coordinamento multidisciplinare capace di accompagnare l'intero ciclo di vita dell'innovazione: dalla valutazione preliminare della tecnologia alla sua introduzione nei processi assistenziali, sino al monitoraggio degli eventi avversi, alla gestione del contenzioso e alla conseguente revisione organizzativa.

L'obiettivo è trasformare la conformità normativa da adempimento prevalentemente formale in strumento di governo anticipatorio del rischio, realizzando un sistema nel quale innovazione, sicurezza, qualità delle cure e responsabilità organizzativa costituiscano componenti di un unico processo decisionale.

Parole chiave: sicurezza delle cure; clinical risk management; intelligenza artificiale; sanità digitale; governance sanitaria; responsabilità sanitaria; telemedicina; dati sanitari; AI Act; EHDS.

1. Introduzione: dalla sicurezza clinica alla sicurezza del sistema sanitario digitale

Sito web: www.ratioiuris.it
Informazioni: info@ratioiuris.it
Redazione: redazione@ratioiuris.it
Coordinamento Generale: Avv. Maria Antonietta Bozza
Coordinamento Editoriale: Avv. Stenio Salzano

ISSN 2420-7888

La sicurezza delle cure costituisce oggi uno dei principali paradigmi attraverso i quali valutare la qualità di un'organizzazione sanitaria. La progressiva complessità dei percorsi assistenziali, la multidisciplinarietà delle prestazioni, l'integrazione tra ospedale e territorio e, soprattutto, la crescente presenza della tecnologia all'interno dei processi diagnostici, terapeutici e organizzativi impongono tuttavia una revisione della tradizionale nozione di rischio clinico.

L'Organizzazione Mondiale della Sanità ha collocato la *patient safety* tra le componenti fondamentali della qualità dell'assistenza, elaborando nel *Global Patient Safety Action Plan 2021–2030* un modello nel quale la prevenzione del danno evitabile richiede interventi non soltanto sul singolo professionista, ma sull'organizzazione, sulla leadership, sui processi, sulle tecnologie e sulla cultura della sicurezza.[1]

Tale impostazione appare particolarmente coerente con il sistema italiano delineato dalla legge 8 marzo 2017, n. 24. L'art. 1 della legge stabilisce infatti che la sicurezza delle cure è parte costitutiva del diritto alla salute e deve essere perseguita nell'interesse dell'individuo e della collettività. La disposizione assume un significato sistematico particolarmente rilevante perché sposta l'asse della sicurezza dalla dimensione esclusivamente professionale a quella organizzativa.

La sicurezza non dipende soltanto dalla corretta esecuzione della singola prestazione sanitaria. Essa dipende dall'organizzazione dei percorsi, dalla comunicazione tra professionisti, dalla disponibilità delle informazioni cliniche, dalla corretta allocazione delle competenze, dalla qualità delle tecnologie impiegate e, sempre più frequentemente, dall'affidabilità dei sistemi informatici e algoritmici che concorrono alla decisione clinica.

La trasformazione digitale rende pertanto insufficiente un modello di risk management concentrato prevalentemente sugli eventi avversi clinici. Al rischio clinico tradizionale si affiancano il rischio organizzativo, quello digitale e informativo, il rischio derivante dall'utilizzo di sistemi algoritmici e quello connesso alla sicurezza cibernetica. Si tratta di dimensioni tra loro strettamente interdipendenti. Un errore diagnostico può derivare dalla condotta del professionista, ma anche dall'incompletezza del dato disponibile, da un problema di interoperabilità, dall'erronea configurazione di un software, da un output algoritmico non adeguatamente verificato o da un difetto organizzativo nella distribuzione delle responsabilità.

Ne deriva la necessità di passare dal *clinical risk management* a una più ampia **governance integrata del rischio sanitario e dell'innovazione**.

2. La sicurezza delle cure come funzione organizzativa

La legge n. 24/2017 ha segnato il definitivo riconoscimento della natura organizzativa della sicurezza delle cure. L'art. 1, comma 2, stabilisce che essa si realizza anche mediante l'insieme delle attività finalizzate alla prevenzione e alla gestione del rischio connesso all'erogazione delle prestazioni sanitarie e mediante l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative.[2]

Particolarmente significativa è l'estensione delle attività di prevenzione del rischio a tutto il personale, compresi i liberi professionisti operanti in regime di convenzione con il Servizio sanitario nazionale. La disposizione suggerisce una lettura della sicurezza quale **funzione trasversale dell'organizzazione**.

Il rischio non appartiene infatti esclusivamente alla struttura di risk management. Esso attraversa la direzione sanitaria e quella amministrativa, coinvolge i sistemi informativi e l'ingegneria clinica,

interessa le unità operative e gli uffici legali e interseca inevitabilmente le funzioni deputate alla protezione dei dati e alla sicurezza informatica. La sicurezza delle cure deve quindi essere interpretata come risultato dell'interazione tra una pluralità di strutture, professionalità e responsabilità.

AGENAS, nell'ambito delle attività dell'Osservatorio nazionale delle buone pratiche sulla sicurezza nella sanità, ha evidenziato il rapporto tra monitoraggio degli eventi avversi, contenzioso, sicurezza delle cure e sostenibilità del sistema.[3] Il punto assume rilievo anche sotto il profilo della responsabilità della struttura sanitaria.

La responsabilità organizzativa non coincide necessariamente con l'errore del singolo sanitario. Una prestazione tecnicamente corretta può inserirsi in un percorso organizzativamente inadeguato; viceversa, una struttura capace di dimostrare l'esistenza di procedure, sistemi di monitoraggio, formazione, audit e meccanismi di controllo dispone di strumenti più efficaci tanto per prevenire il danno quanto per ricostruire ex post le cause di un evento.

La sicurezza assume così la configurazione di un processo circolare, nel quale l'identificazione del rischio precede l'attività preventiva e l'eventuale verificarsi dell'evento costituisce il punto di partenza per l'analisi delle cause, la gestione delle conseguenze e l'apprendimento organizzativo. Anche il contenzioso, in questa prospettiva, dovrebbe essere considerato non soltanto una conseguenza economico-giuridica dell'evento avverso, ma una fonte informativa capace di orientare la revisione delle procedure e delle scelte di governo clinico.

3. Innovazione tecnologica e nuove categorie di rischio sanitario

L'introduzione delle tecnologie digitali modifica profondamente tale scenario. Telemedicina, sistemi di supporto alla decisione clinica, dispositivi medici con componenti software, sistemi predittivi, algoritmi di prioritizzazione e strumenti di intelligenza artificiale generativa introducono nuovi soggetti, nuove interazioni e nuove possibili fonti di errore.

Il rischio sanitario diviene pertanto un rischio **socio-tecnico**, poiché l'evento dannoso può dipendere dall'interazione tra professionista, organizzazione e tecnologia senza essere integralmente riconducibile ad alcuno di tali elementi isolatamente considerato.

L'intelligenza artificiale rende particolarmente evidente il fenomeno. Un sistema algoritmico utilizzato nella diagnosi può produrre un risultato tecnicamente errato; può tuttavia verificarsi anche un utilizzo improprio di un output formalmente corretto, un eccessivo affidamento dell'operatore sul sistema (*automation bias*), un impiego su una popolazione diversa da quella sulla quale il modello è stato validato o una progressiva alterazione delle performance conseguente al mutamento dei dati.

La letteratura europea ha evidenziato come la regolazione dell'IA sanitaria sia ormai costituita da una pluralità di fonti riguardanti intelligenza artificiale, dispositivi medici, dati personali, diritti fondamentali e organizzazione sanitaria.[4] Ne consegue che la sicurezza dell'innovazione non può essere affidata esclusivamente alla valutazione tecnica del prodotto.

La valutazione dovrebbe investire contemporaneamente l'appropriatezza clinica della tecnologia, la sua compatibilità con l'organizzazione nella quale viene introdotta, la sostenibilità giuridica del relativo utilizzo e la concreta capacità dello strumento di integrarsi nei percorsi assistenziali senza introdurre nuovi fattori di rischio.

4. AI Act e governo dell'intelligenza artificiale sanitaria

Sito web: www.ratioiuris.it
Informazioni: info@ratioiuris.it
Redazione: redazione@ratioiuris.it
Coordinamento Generale: Avv. Maria Antonietta Bozza
Coordinamento Editoriale: Avv. Stenio Salzano

ISSN 2420-7888

Il Regolamento (UE) 2024/1689 introduce nell'ordinamento europeo un sistema di regolazione dell'intelligenza artificiale fondato sulla graduazione del rischio. Per il settore sanitario assume particolare rilevanza la disciplina dei sistemi di IA qualificabili come ad alto rischio, tra i quali possono rientrare, alle condizioni previste dal Regolamento, sistemi incorporati in prodotti soggetti alla normativa europea di armonizzazione, compresi determinati dispositivi medici.

Il punto centrale, nella prospettiva delle organizzazioni sanitarie, è che il governo dell'IA non può esaurirsi nella conformità del produttore. Anche l'organizzazione che utilizza professionalmente il sistema è chiamata a governarne concretamente l'impiego.

Ciò comporta anzitutto la necessità di conoscere quali sistemi algoritmici siano effettivamente utilizzati all'interno dell'azienda, comprenderne la funzione e il livello di rischio e individuare chiaramente i soggetti responsabili dei relativi processi. A questa preliminare attività di ricognizione deve accompagnarsi la definizione delle modalità attraverso le quali viene esercitata la supervisione umana, nonché un'adeguata formazione degli operatori. Il sistema deve inoltre essere inserito in un processo di monitoraggio che consenta di verificare gli output prodotti, ricostruire il suo utilizzo, intercettare eventuali incidenti e prevedere procedure di sospensione o revisione qualora emergano anomalie significative.

La **human oversight** assume, in sanità, una valenza che trascende il mero adempimento tecnico. La supervisione umana rappresenta il punto di collegamento tra sicurezza tecnologica, autonomia professionale e responsabilità sanitaria.

Il professionista non dovrebbe trasformarsi in mero esecutore dell'algoritmo; al tempo stesso, non appare sufficiente affermare genericamente che la decisione finale rimane umana. È necessario che l'organizzazione garantisca concretamente al professionista le condizioni informative e formative per comprendere il significato dell'output, valutarne criticamente l'attendibilità e, quando necessario, discostarsene.

La legislazione italiana in materia di intelligenza artificiale rafforza questa impostazione, inserendo l'impiego dell'IA in sanità all'interno di un quadro orientato al miglioramento del sistema sanitario e alla tutela della persona. Si configura pertanto una vera **responsabilità organizzativa nell'introduzione dell'algoritmo**, che precede e accompagna la responsabilità connessa al suo utilizzo nel singolo caso clinico.

5. Dati sanitari, interoperabilità ed EHDS

Non esiste sanità digitale senza governo del dato. La qualità dell'algoritmo, della telemedicina e, più in generale, della decisione clinica digitale dipende dalla disponibilità, accuratezza, completezza, interoperabilità e sicurezza delle informazioni utilizzate.

Il Regolamento (UE) 2025/327 sullo European Health Data Space rappresenta, sotto questo profilo, un passaggio fondamentale. L'EHDS mira a costruire un quadro europeo comune per l'accesso e lo scambio dei dati sanitari elettronici, distinguendo tra uso primario, direttamente connesso all'assistenza sanitaria, e uso secondario, relativo, tra l'altro, a ricerca, innovazione, programmazione e attività regolatorie.[5]

Il Regolamento introduce inoltre un quadro armonizzato per i sistemi di cartella clinica elettronica e pone l'interoperabilità al centro della futura infrastruttura sanitaria europea.

Sito web: www.ratioiuris.it
Informazioni: info@ratioiuris.it
Redazione: redazione@ratioiuris.it
Coordinamento Generale: Avv. Maria Antonietta Bozza
Coordinamento Editoriale: Avv. Stenio Salzano

ISSN 2420-7888

La conseguenza organizzativa è rilevante. La gestione del dato sanitario non può essere considerata una questione esclusivamente informatica, né può essere ricondotta soltanto alla protezione dei dati personali. Il medesimo dato costituisce infatti oggetto di tutela giuridica e, contemporaneamente, elemento della documentazione sanitaria, strumento della continuità assistenziale, fattore determinante per la sicurezza delle cure, possibile input di sistemi algoritmici e risorsa per la ricerca e la programmazione sanitaria.

La governance del dato deve pertanto essere collegata alla governance clinica. Un'informazione incompleta, inesatta o non tempestivamente disponibile può determinare un rischio assistenziale non meno significativo di quello derivante da una procedura clinica inappropriata.

L'OECD ha evidenziato come sistemi integrati di informazione sanitaria siano essenziali per qualità, sicurezza, ricerca, innovazione e valutazione delle performance, sottolineando al contempo la necessità di conciliare disponibilità dei dati, interoperabilità, privacy e sicurezza.[6]

6. Telemedicina e continuità assistenziale

Un ulteriore banco di prova della governance integrata è rappresentato dalla telemedicina.

Il D.M. 23 maggio 2022, n. 77, nel ridisegnare i modelli dell'assistenza territoriale, inserisce gli strumenti digitali all'interno dei nuovi percorsi di presa in carico. Le Centrali Operative Territoriali rappresentano uno dei principali snodi del nuovo modello, assicurando il coordinamento tra professionisti e differenti setting assistenziali. Il modello territoriale collega COT, Case della Comunità, assistenza domiciliare, Ospedali di Comunità e servizi ospedalieri, attribuendo alle infrastrutture digitali un ruolo essenziale nel garantire continuità e integrazione.[7]

AGENAS ha inoltre assunto specifiche funzioni attuative, nell'ambito della Missione 6 del PNRR, con riferimento alla telemedicina e alle Centrali Operative Territoriali.[8]

La prestazione a distanza non elimina tuttavia il rischio clinico, ma ne modifica la struttura. L'organizzazione deve valutare preliminarmente quando la modalità a distanza sia appropriata rispetto alle condizioni del paziente e alla natura della prestazione; deve assicurare una corretta identificazione dell'assistito e la disponibilità di informazioni cliniche sufficienti; deve inoltre garantire che l'utilizzo della tecnologia non interrompa la continuità del percorso e che sia possibile, quando necessario, il passaggio tempestivo dalla modalità remota a quella in presenza.

La telemedicina non dovrebbe quindi essere considerata una semplice modalità tecnologica alternativa alla prestazione tradizionale, bensì un **processo clinico-organizzativo autonomamente governato**, inserito nella più ampia politica aziendale di sicurezza.

7. Il limite dell'attuale modello organizzativo: la governance per silos

Uno dei principali problemi delle aziende sanitarie contemporanee consiste nella frammentazione delle competenze.

Il rischio clinico viene normalmente governato attraverso strutture dedicate; il contenzioso è affidato agli uffici legali; la protezione dei dati ricade nell'ambito delle funzioni previste dalla disciplina europea; la cybersecurity e l'infrastruttura tecnologica sono prevalentemente presidiate dai sistemi informativi, mentre l'ingegneria clinica, le strutture deputate alla qualità, alla formazione e alla valutazione delle tecnologie intervengono secondo le rispettive attribuzioni.

Sito web: www.ratioiuris.it
Informazioni: info@ratioiuris.it
Redazione: redazione@ratioiuris.it
Coordinamento Generale: Avv. Maria Antonietta Bozza
Coordinamento Editoriale: Avv. Stenio Salzano

ISSN 2420-7888

Una simile distribuzione delle competenze è fisiologica e, sotto molti aspetti, indispensabile. Diviene tuttavia problematica quando alla specializzazione delle funzioni non corrisponde un adeguato livello di coordinamento.

Lo stesso evento può presentare contemporaneamente implicazioni cliniche, organizzative, tecnologiche, giuridiche e informative. Si consideri, ad esempio, l'introduzione di un sistema di intelligenza artificiale destinato alla prioritizzazione di esami diagnostici. La decisione interessa l'appropriatezza clinica e la sicurezza del paziente, ma coinvolge contemporaneamente la disciplina dell'AI Act e, ove ne ricorrano i presupposti, quella dei dispositivi medici; incide sul trattamento dei dati e sulla cybersecurity; produce conseguenze sul piano della responsabilità professionale e organizzativa; richiede formazione degli operatori e interagisce con le procedure di acquisizione della tecnologia e con l'organizzazione del personale.

Una governance frammentata determina quindi il rischio che ciascuna struttura valuti correttamente una porzione del problema senza che venga adeguatamente considerato il **rischio complessivo del processo**.

8. Un modello di Governance Integrata della Sicurezza e dell'Innovazione

Alla luce delle criticità evidenziate, appare possibile delineare un modello di **Governance Integrata della Sicurezza e dell'Innovazione (GISI)**.

La proposta non implica necessariamente la creazione di un'ulteriore struttura amministrativa. L'obiettivo è piuttosto quello di costruire una funzione stabile di coordinamento capace di mettere in relazione competenze che già esistono all'interno dell'organizzazione.

Il modello dovrebbe trovare il proprio centro nella Direzione strategica e collegare stabilmente le funzioni di risk management e direzione sanitaria con quelle legali, informatiche, di ingegneria clinica, protezione dei dati, cybersecurity, qualità e valutazione delle tecnologie, assicurando altresì il coinvolgimento dei professionisti clinici direttamente interessati. La Direzione strategica conserverebbe la responsabilità del governo complessivo, facendo confluire le differenti valutazioni specialistiche in un processo decisionale unitario.

8.1. La mappatura dinamica del rischio

Il primo momento del modello dovrebbe essere costituito dalla conoscenza sistematica dei rischi presenti nell'organizzazione. L'azienda dovrebbe disporre di una mappatura dinamica che metta in relazione i processi clinici maggiormente esposti con le tecnologie digitali effettivamente utilizzate, i sistemi di intelligenza artificiale, i flussi informativi critici e le informazioni provenienti dagli eventi avversi, dagli incidenti informatici, dal contenzioso e dalle segnalazioni degli operatori.

Il valore aggiunto di questa mappatura consisterebbe proprio nella capacità di integrare informazioni normalmente conservate in sistemi differenti. Un aumento delle richieste risarcitorie in una determinata area, ad esempio, potrebbe assumere un significato diverso qualora venisse correlato temporalmente all'introduzione di una nuova tecnologia o alla modifica di un processo informativo.

8.2. La valutazione preventiva dell'innovazione

ISSN 2420-7888

Il secondo momento riguarda la valutazione preventiva. Le tecnologie capaci di incidere significativamente sulla decisione clinica non dovrebbero essere valutate soltanto sotto il profilo delle prestazioni tecniche o economiche.

Accanto alle metodologie proprie dell'Health Technology Assessment appare utile introdurre uno specifico **Health Innovation Risk Assessment (HIRA)**, destinato a valutare in maniera congiunta la sicurezza clinica della tecnologia, la conformità giuridica, la governance dei dati, la sicurezza informatica, l'effettività della supervisione umana e l'impatto sull'organizzazione.

La valutazione assumerebbe così una natura autenticamente multidimensionale. L'interrogativo non sarebbe soltanto se una tecnologia funzioni, ma se essa possa funzionare in sicurezza **all'interno di quella specifica organizzazione sanitaria**.

8.3. L'introduzione controllata dell'innovazione

La valutazione positiva dovrebbe essere seguita da una fase di introduzione controllata. L'organizzazione dovrebbe definire preventivamente le finalità per le quali la tecnologia può essere impiegata, la popolazione di riferimento, i professionisti autorizzati all'utilizzo e le modalità attraverso le quali l'attività viene documentata.

Particolare attenzione dovrebbe essere riservata alla supervisione umana e alla gestione delle anomalie. Devono risultare comprensibili tanto le condizioni nelle quali il professionista può utilizzare lo strumento quanto quelle nelle quali il suo utilizzo deve essere sospeso o sottoposto a rivalutazione.

In questa prospettiva, il protocollo aziendale non costituisce un mero adempimento documentale, ma diviene lo strumento attraverso il quale la tecnologia viene inserita nel sistema delle responsabilità organizzative.

8.4. Il monitoraggio successivo

La governance non può terminare con l'autorizzazione all'utilizzo. Una tecnologia inizialmente affidabile può produrre nel tempo risultati differenti in ragione della modifica dei dati, dell'evoluzione dei processi o delle modalità concrete attraverso le quali viene utilizzata dagli operatori.

Il monitoraggio dovrebbe quindi mettere in relazione incidenti e *near miss* con eventuali deviazioni dagli output attesi, problemi di interoperabilità, segnalazioni degli operatori, reclami dei pazienti e contenzioso. L'integrazione di queste fonti permetterebbe di individuare precocemente segnali che, se considerati separatamente, potrebbero apparire privi di particolare significato.

8.5. L'apprendimento organizzativo

L'ultima fase chiude il ciclo della governance. L'evento avverso non deve essere considerato soltanto come fallimento del sistema, ma come fonte di conoscenza sulla sua vulnerabilità.

Il modello proposto può essere concettualmente rappresentato attraverso la sequenza **Map – Assess – Authorise – Monitor – Learn**. Non si tratta di una successione rigidamente lineare, ma di un ciclo continuo nel quale le informazioni ottenute dal monitoraggio e dall'analisi degli eventi modificano progressivamente la mappatura iniziale e determinano nuove valutazioni.

È proprio questa circolarità a segnare il passaggio da una governance prevalentemente reattiva a una **governance anticipatoria del rischio**.

Sito web: www.ratioiuris.it
Informazioni: info@ratioiuris.it
Redazione: redazione@ratioiuris.it
Coordinamento Generale: Avv. Maria Antonietta Bozza
Coordinamento Editoriale: Avv. Stenio Salzano

ISSN 2420-7888

9. Il ruolo della funzione giuridica nella clinical governance

Nel modello delineato assume particolare importanza la componente giuridica.

Tradizionalmente, il giurista entra nel processo sanitario quando il conflitto è già sorto, attraverso la gestione del reclamo, della richiesta risarcitoria o del procedimento giudiziario. La crescente complessità normativa e tecnologica rende tale impostazione insufficiente.

La funzione giuridica dovrebbe intervenire in una fase antecedente all'evento, concorrendo alla progettazione dei processi organizzativi e all'analisi preventiva delle conseguenze normative derivanti dall'introduzione delle innovazioni.

Può così delinearsi un vero e proprio **legal risk management sanitario**, nel quale l'analisi della normativa applicabile si integra con la verifica dei modelli organizzativi, con la predisposizione dei protocolli, con l'individuazione delle aree di responsabilità e con la formazione dei professionisti. Allo stesso tempo, le informazioni provenienti dal contenzioso devono essere restituite al risk management e alla Direzione strategica affinché possano essere utilizzate nella revisione dei processi.

Il passaggio concettuale è significativo. Il diritto non interviene soltanto per attribuire responsabilità dopo che il danno si è verificato, ma concorre a **progettare organizzazioni capaci di prevenirlo**.

10. Dal contenzioso all'apprendimento organizzativo

Una delle componenti più rilevanti del modello proposto riguarda l'utilizzo del contenzioso come indicatore di rischio.

Ogni richiesta risarcitoria contiene informazioni sul funzionamento dell'organizzazione. Considerati singolarmente, i procedimenti giudiziari possono apparire eventi autonomi; analizzati in forma aggregata, possono invece evidenziare la concentrazione delle controversie in determinate unità operative, la ricorrenza di specifiche tipologie di evento, criticità nella documentazione sanitaria, ritardi diagnostici, problemi nella comunicazione con il paziente, carenze nella gestione del consenso informato o disfunzioni nella continuità assistenziale.

A tali elementi si aggiungono oggi i rischi connessi alle tecnologie digitali. L'analisi del contenzioso potrebbe, ad esempio, consentire di individuare una correlazione tra determinate criticità assistenziali e problemi di interoperabilità, sistemi di supporto decisionale o nuove modalità di erogazione della prestazione.

Il fascicolo giudiziario può così trasformarsi in una fonte di *organisational learning*. In questa prospettiva, appare utile prevedere una **Litigation Safety Review**, attraverso la quale i casi conclusi o comunque particolarmente significativi vengano periodicamente esaminati congiuntamente dalla funzione legale e dal risk management, con il coinvolgimento delle strutture cliniche interessate quando necessario.

Si determina in tal modo una circolarità virtuosa nella quale l'evento produce conoscenza, il contenzioso contribuisce alla ricostruzione delle vulnerabilità del sistema e le informazioni acquisite vengono trasformate in interventi organizzativi e misure preventive. La gestione del contenzioso cessa così di essere esclusivamente difensiva e diviene parte integrante della politica aziendale di sicurezza delle cure.

11. La misurabilità della governance integrata

Sito web: www.ratioiuris.it
Informazioni: info@ratioiuris.it
Redazione: redazione@ratioiuris.it
Coordinamento Generale: Avv. Maria Antonietta Bozza
Coordinamento Editoriale: Avv. Stenio Salzano

ISSN 2420-7888

Un modello organizzativo può essere considerato efficace soltanto quando i suoi risultati sono verificabili.

La governance integrata richiede quindi indicatori capaci di mettere in relazione informazioni tradizionalmente separate. Non è sufficiente conoscere il numero complessivo degli eventi avversi o delle richieste risarcitorie; occorre verificare la loro distribuzione per area assistenziale e tipologia di evento, la presenza di *near miss*, il numero e la natura delle tecnologie sottoposte a valutazione preventiva, la consistenza dei sistemi di intelligenza artificiale effettivamente utilizzati e il livello di formazione dei professionisti coinvolti.

Particolare rilevanza dovrebbe essere attribuita agli incidenti digitali suscettibili di produrre conseguenze cliniche e alle criticità di interoperabilità, verificando altresì quali azioni correttive siano state effettivamente attuate a seguito degli audit, degli eventi avversi o del contenzioso.

Tali informazioni potrebbero confluire in una **dashboard integrata del rischio aziendale** destinata alla Direzione strategica. La finalità non sarebbe quella di incrementare gli adempimenti burocratici, bensì di trasformare dati già disponibili nell'organizzazione in conoscenza utile alla decisione.

La tecnologia verrebbe così utilizzata non soltanto come possibile fonte di nuovi rischi, ma anche come strumento per identificarli e governarli.

12. Discussione

Il modello proposto muove dalla constatazione che il sistema sanitario contemporaneo non può più essere governato mediante categorie organizzative concepite quando tecnologia, attività clinica e gestione del dato costituivano ambiti relativamente separabili.

La digitalizzazione ha progressivamente eliminato tale separazione.

La sicurezza del paziente dipende ormai anche dalla sicurezza e dalla qualità del dato; la qualità della decisione clinica può essere condizionata dall'affidabilità dell'algoritmo; la continuità assistenziale dipende sempre più dall'interoperabilità; la responsabilità del professionista può essere influenzata dalle scelte tecnologiche e organizzative compiute dalla struttura.

Il paradigma dovrebbe quindi evolvere dal tradizionale *clinical risk management* verso una più ampia **integrated healthcare risk governance**.

Il vantaggio del modello integrato si manifesta innanzitutto sul piano clinico, poiché l'interconnessione delle informazioni può favorire una migliore prevenzione degli eventi avversi. Ma assume rilievo anche sul piano giuridico e organizzativo, consentendo alla struttura di documentare l'esistenza di processi strutturati di identificazione, valutazione, monitoraggio e controllo del rischio.

Ciò assume particolare rilevanza nell'era dell'intelligenza artificiale, nella quale la ricostruzione delle responsabilità potrà interessare una pluralità di soggetti collocati lungo la catena tecnologica e assistenziale, dal produttore e dal fornitore sino all'organizzazione sanitaria e al professionista che utilizza il sistema.

La governance integrata non determina una diluizione delle responsabilità. Al contrario, dovrebbe renderne più chiara l'allocazione, consentendo di distinguere ciò che dipende dalla tecnologia, ciò che appartiene alla scelta professionale e ciò che costituisce espressione dell'organizzazione.

Sito web: www.ratioiuris.it
Informazioni: info@ratioiuris.it
Redazione: redazione@ratioiuris.it
Coordinamento Generale: Avv. Maria Antonietta Bozza
Coordinamento Editoriale: Avv. Stenio Salzano

ISSN 2420-7888

13. Conclusioni

La trasformazione digitale della sanità impone di ripensare il significato stesso di sicurezza delle cure.

L'innovazione non può essere considerata sicura per il solo fatto di essere tecnologicamente avanzata o formalmente conforme alle norme applicabili. Essa è sicura quando l'organizzazione sanitaria è in grado di conoscerla, valutarla, integrarla nei processi assistenziali, monitorarne gli effetti e intervenire tempestivamente quando emergono criticità.

La sicurezza delle cure, il governo dell'intelligenza artificiale, la telemedicina, la protezione e la qualità dei dati, la cybersecurity e la gestione del contenzioso costituiscono pertanto differenti manifestazioni di un medesimo problema: **la capacità dell'organizzazione sanitaria di governare la complessità**.

Il modello di governance integrata proposto mira a superare la frammentazione delle competenze senza eliminarne la necessaria specializzazione. L'elemento centrale non risiede nella creazione di una nuova struttura burocratica, bensì nella costruzione di un processo stabile di coordinamento nel quale le differenti competenze possano concorrere alla formazione della decisione aziendale.

La vera innovazione organizzativa consiste, in definitiva, nel passaggio da un sistema che reagisce al rischio dopo che questo si è manifestato a un sistema capace di **anticiparlo, misurarlo e apprendere dai propri errori**.

In questa prospettiva, diritto, medicina, tecnologia e organizzazione non rappresentano discipline parallele, ma componenti di un'unica e moderna politica aziendale di sicurezza delle cure.

NOTE

[1] World Health Organization, *Global Patient Safety Action Plan 2021–2030: Towards Eliminating Avoidable Harm in Health Care*, Geneva, WHO, 2021.

[2] Legge 8 marzo 2017, n. 24, *Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie*, art. 1.

[3] AGENAS, documentazione istituzionale in materia di rischio clinico e sicurezza del paziente e attività dell'Osservatorio nazionale delle buone pratiche sulla sicurezza nella sanità.

[4] R. van Kessel et al., *Mapping the regulatory landscape for artificial intelligence in health within the European Union*, **npj Digital Medicine**, 2024, 7, 229.

[5] Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari (European Health Data Space – EHDS).

[6] OECD, *Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance*, OECD Publishing, Paris, 2022.

[7] Decreto del Ministro della salute 23 maggio 2022, n. 77, *Regolamento recante la definizione di modelli e standard per lo sviluppo dell'assistenza territoriale nel Servizio sanitario nazionale*.

[8] AGENAS, *Report nazionale di sintesi dei risultati del Monitoraggio DM 77/2022 – II semestre 2024*, Roma, 2025.

Sito web: www.ratioiuris.it
Informazioni: info@ratioiuris.it
Redazione: redazione@ratioiuris.it
Coordinamento Generale: Avv. Maria Antonietta Bozza
Coordinamento Editoriale: Avv. Stenio Salzano

[9] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (*Artificial Intelligence Act*).

[10] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

[11] Legge 23 settembre 2025, n. 132, *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*.

[12] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.

[13] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici.

[14] M. Panagioti et al., *Prevalence, severity, and nature of preventable patient harm across medical care settings: systematic review and meta-analysis*, **BMJ**, 2019, 366, l4185.

[15] L. Slawomirski, A. Auraaen, N. Klazinga, *The Economics of Patient Safety in Primary and Ambulatory Care: Flying Blind*, OECD Health Working Papers, No. 106, OECD Publishing, Paris, 2018.

BIBLIOGRAFIA

AGENAS, *Rischio clinico e sicurezza del paziente*, Agenzia Nazionale per i Servizi Sanitari Regionali, Roma.

AGENAS, *Report nazionale di sintesi dei risultati del Monitoraggio DM 77/2022 – II semestre 2024*, Roma, 2025.

OECD, *Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance*, OECD Publishing, Paris, 2022.

Panagioti M., Khan K., Keers R.N., Abuzour A., Phipps D., Kontopantelis E. et al., *Prevalence, severity, and nature of preventable patient harm across medical care settings: systematic review and meta-analysis*, **BMJ**, 2019, 366, l4185.

Slawomirski L., Auraaen A., Klazinga N., *The Economics of Patient Safety in Primary and Ambulatory Care: Flying Blind*, OECD Health Working Papers, No. 106, OECD Publishing, Paris, 2018.

van Kessel R. et al., *Mapping the regulatory landscape for artificial intelligence in health within the European Union*, **npj Digital Medicine**, 2024, 7, 229.

World Health Organization, *Global Patient Safety Action Plan 2021–2030: Towards Eliminating Avoidable Harm in Health Care*, WHO, Geneva, 2021.

Fonti normative

Legge 8 marzo 2017, n. 24, *Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie*.

D.M. 23 maggio 2022, n. 77, *Regolamento recante la definizione di modelli e standard per lo sviluppo dell'assistenza territoriale nel Servizio sanitario nazionale*.

ISSN 2420-7888

Legge 23 settembre 2025, n. 132, *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*.

Regolamento (UE) 2016/679, *General Data Protection Regulation*.

Regolamento (UE) 2017/745 relativo ai dispositivi medici.

Direttiva (UE) 2022/2555, *NIS 2 Directive*.

Regolamento (UE) 2024/1689, *Artificial Intelligence Act*.

Regolamento (UE) 2025/327, *European Health Data Space*.

Sito web: www.ratioiuris.it
Informazioni: info@ratioiuris.it
Redazione: redazione@ratioiuris.it
Coordinamento Generale: Avv. Maria Antonietta Bozza
Coordinamento Editoriale: Avv. Stenio Salzano