Sicurezza informatica in sanità: GDPR, rischio cyber e governance dei dati

Questo articolo fa parte di una serie di approfondimenti dedicati alla sicurezza informatica in sanità, con l'obiettivo di analizzare il complesso rapporto tra trasformazione digitale, protezione dei dati personali e governance dei sistemi informativi sanitari. In particolare, il contributo esamina il quadro normativo europeo, con focus sul GDPR, e approfondisce il ruolo degli standard internazionali nella gestione del rischio informatico e nella tutela delle informazioni sanitarie.

Negli ultimi anni il settore sanitario è stato interessato da un processo di trasformazione strutturale profondamente influenzato dallo sviluppo delle tecnologie digitali e dalla progressiva informatizzazione dei servizi pubblici. L'introduzione di sistemi informativi sanitari, piattaforme digitali per la gestione delle prestazioni e strumenti avanzati per la raccolta, l'archiviazione e l'elaborazione dei dati clinici ha determinato un significativo miglioramento dell'efficienza organizzativa delle strutture sanitarie, favorendo una maggiore integrazione tra i diversi attori del sistema e consentendo una gestione più tempestiva e coordinata delle informazioni relative ai pazienti.

Parallelamente ai benefici derivanti dal processo di digitalizzazione, sono tuttavia emerse nuove criticità connesse alla sicurezza delle informazioni e alla protezione dei dati personali. Le organizzazioni sanitarie trattano quotidianamente una quantità estremamente rilevante di informazioni appartenenti alle cosiddette categorie particolari di dati personali, tra cui rientrano i dati relativi alla salute, che per la loro natura sensibile

richiedono un livello di tutela particolarmente elevato. La crescente interconnessione delle infrastrutture digitali, unita alla diffusione di tecnologie informatiche sempre più complesse, ha infatti ampliato la superficie di esposizione ai rischi informatici, rendendo i sistemi sanitari potenzialmente vulnerabili ad accessi non autorizzati, perdita o alterazione dei dati, nonché ad attacchi informatici sempre più sofisticati.

In tale contesto assume una rilevanza centrale il tema della gestione del rischio informatico, che rappresenta uno degli strumenti fondamentali per garantire la sicurezza delle informazioni, la tutela dei diritti e delle libertà fondamentali degli interessati. La sicurezza informatica, a questo punto, non può essere considerata esclusivamente come una questione di natura tecnica, ma richiede l'adozione di un approccio multidisciplinare che integri aspetti giuridici, organizzativi e gestionali all'interno dei processi decisionali delle organizzazioni.

Il quadro normativo europeo ha progressivamente rafforzato l'attenzione verso tali problematiche, in particolare attraverso l'adozione del Regolamento (UE) 2016/679, noto come *General Data Protection Regulation* (GDPR), che ha introdotto un modello di protezione dei dati personali fondato sul principio di responsabilizzazione del titolare del trattamento. Tale principio impone alle organizzazioni l'obbligo di adottare misure tecniche e organizzative adeguate al rischio, nonché di implementare strumenti di *governance* in grado di garantire un trattamento dei dati conforme ai principi di sicurezza, integrità e riservatezza.

In questo scenario, inoltre, assumono rilievo anche gli standard internazionali in materia di sicurezza delle informazioni, tra cui la ISO/IEC 27001:2022 abbinata al suo allegato A, che definisce i requisiti per l'implementazione di un sistema di gestione della sicurezza delle informazioni (*Information Security Management System* – ISMS). Tale *standard*

fornisce un modello organizzativo strutturato volto a garantire un approccio sistematico alla protezione delle informazioni, basato sull'identificazione, sulla valutazione e sul trattamento dei rischi informatici.

Accanto a ciò, un contributo rilevante è offerto anche dalla ISO/IEC 27005:2022, che fornisce linee guida operative per l'implementazione dei controlli di sicurezza delle informazioni a supporto dei requisiti previsti dalla ISO/IEC 27001 e che disciplina in modo specifico i processi di gestione del rischio informatico all'interno delle organizzazioni. Va considerata, inoltre, anche la ISO 22301:2019, che attraverso i concetti di continuità operativa e resilienza rappresenta la capacità di un'organizzazione di prevenire, assorbire e gestire eventi dirompenti, garantendo il mantenimento dei prodotti e dei servizi essenziali a livelli ammissibili anche in condizioni di crisi.

La norma, infatti, propone un approccio sistemico e strutturato alla continuità operativa, basato sull'implementazione di un Sistema di Gestione della Continuità Operativa (*Business Continuity Management System* – BCMS), volto a pianificare, attuare e migliorare in modo continuo le capacità di risposta e recupero dell'organizzazione.

Alla luce di tali premesse, l'obiettivo del presente lavoro è quello di analizzare il ruolo della gestione del rischio informatico nel settore sanitario, con particolare riferimento all'integrazione tra il quadro normativo europeo in materia di protezione dei dati personali e i modelli organizzativi previsti dagli *standard* internazionali di sicurezza delle informazioni.

Dunque, il white paper in questione si articola in più capitoli. In primo luogo, viene delineato il quadro normativo relativo alla protezione dei dati personali, con particolare attenzione al trattamento dei dati sanitari e ai principi

fondamentali introdotti dal GDPR. Successivamente l'analisi si concentra sugli strumenti di gestione della sicurezza delle informazioni, esaminando il funzionamento dei sistemi di gestione della sicurezza informatica e il ruolo degli standard internazionali.

In seguito, vengono approfonditi gli strumenti di prevenzione dei rischi previsti dalla normativa europea, tra cui la valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment*), nonché le principali problematiche annodate alla sicurezza dei sistemi informativi in ambito sanitario. Infine, il white paper si conclude con l'analisi di un caso di incidente informatico, al fine di evidenziare le criticità emerse e le possibili strategie di miglioramento nella gestione della sicurezza delle informazioni.

Attraverso tale percorso, il white paper intende dimostrare come la sicurezza informatica rappresenti, oggi, una componente imprescindibile per il corretto funzionamento di tutte le organizzazioni (in questo caso sanitarie) e per la tutela effettiva dei diritti fondamentali dei cittadini nel mondo digitale.

Il trattamento dei dati sanitari e quadro normativo di riferimento

Prima di esaminare il trattamento dei dati sanitari e quelle che sono le sue condizioni di legittimità, occorre prima riflettere sul significato del termine "dato".

Quest'ultimo si riferisce a qualsiasi rappresentazione, indipendentemente dalla forma assunta, che sia in grado di trasmettere un contenuto conoscitivo[1]con una natura essenzialmente oggettiva[2].

Bisogna, però, riflettere sul concetto di dato inteso come

dato personale, spiegato dal Regolamento (UE) 2016/679[3], nello specifico nell'art. 4, par. 1, n. 1 che intende per «*dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

La possibilità di ricondurre un'informazione a una persona determinata, sia in modo diretto sia mediato, costituisce, dunque, il criterio decisivo per stabilire l'applicazione del Regolamento (UE) 2016/679.

All'interno della nozione di dato personale confluiscono, inoltre, diverse categorie di informazioni. Ad esempio, i dati identificativi consentono l'individuazione immediata dell'interessato e comprendono, tra gli altri, i dati anagrafici, le informazioni bancarie, quelle fiscali e i dati di natura telematica, come l'indirizzo IP.

Oppure, ancora i dati di contatto, invece, permettono di instaurare comunicazioni con l'interessato e includono, ad esempio, l'indirizzo di posta elettronica o il numero telefonico. Particolare rilievo assumono i dati appartenenti a categorie speciali, che si caratterizzano per l'elevata sensibilità delle informazioni trattate. Rientrano in tale ambito i dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'adesione sindacale, nonché lo stato di salute e l'orientamento sessuale della persona. A questi possono essere assimilati quelli giudiziari, genetici e biometrici, ossia i dati ottenuti mediante trattamenti tecnici specifici che consentono l'identificazione univoca dell'individuo, come le

impronte digitali o le caratteristiche della voce.

Restano, esclusi dal suo ambito di operatività i dati anonimi, ossia quelli che non consentono in alcun modo l'individuazione dell'interessato. Al contrario, rientrano nella disciplina europea i dati pseudonimizzati, vale a dire informazioni che, pur essendo state rese parzialmente anonime, possono essere ricondotte a un soggetto specifico mediante l'uso di dati aggiuntivi conservati separatamente.

Dati personali e dati sanitari: definizioni e categorie nel GDPR

Tra i dati appena citati, risulta necessario approfondire la categoria dei dati sanitari, che presenta profili di particolare complessità. Ciò poiché tali dati attengono allo stato di salute fisica e mentale della persona e, per questa ragione, sono suscettibili di incidere in modo significativo sulla dignità, sulla riservatezza e sull'autodeterminazione informativa dell'interessato.

Il primo riferimento normativo rilevante è rappresentato dalla Convenzione di Strasburgo n. 108 del 1981, adottata per garantire la tutela delle persone rispetto al trattamento automatizzato dei dati personali[4]. In tale contesto, l'articolo 6 individua alcune tipologie di dati che richiedono un livello di protezione più elevato, includendo quelli idonei a rivelare lo stato di salute, per i quali il trattamento è consentito solo in presenza di adeguate garanzie previste dall'ordinamento interno.

Un' impostazione quest'ultima che è stata successivamente recepita a livello europeo con la Direttiva 95/46/CE, che ha valorizzato la categoria dei dati sensibili come ambito distinto all'interno dei dati personali[5]. Il legislatore italiano, nel dare attuazione alla direttiva, ha disciplinato

tali dati all'interno del d.lgs. n. 196 del 2003, prevedendo un elenco che, secondo una parte della dottrina, doveva considerarsi chiuso[6]. Tuttavia, la formulazione normativa lasciava spazio a una valutazione elastica, poiché faceva riferimento a dati "idonei a" rivelare determinate informazioni, introducendo un criterio basato sulla potenzialità informativa del dato stesso[7].

All'interno di questo quadro si collocano i dati relativi alla salute, frequentemente qualificati come particolarmente delicati, in ragione della loro capacità di incidere in modo significativo sulla sfera personale dell'interessato.

Proprio per tale motivo, la definizione e l'ambito applicativo dei dati sanitari sono stati oggetto di ampie discussioni in dottrina. Secondo una prima impostazione, l'assenza di una definizione normativa puntuale risponderebbe all'esigenza di lasciare agli operatori un margine di discrezionalità nell'individuare, di volta in volta, quali informazioni possano essere considerate rilevanti ai fini della valutazione dello stato di salute di una persona, privilegiando le finalità del trattamento rispetto al contenuto formale del dato[8]. Altri autori, invece, hanno posto l'accento sull'estensione della categoria, interrogandosi se essa debba comprendere esclusivamente le informazioni che attestano l'esistenza di una patologia oppure anche quelle che consentono soltanto di ipotizzare una condizione di salute[9].

Successivamente, sul piano sovranazionale, il Consiglio d'Europa, con la Raccomandazione (97) 5[10], ha adottato una nozione restrittiva, includendo tra i dati sanitari tutte le informazioni personali direttamente collegate alla salute dell'individuo, nonché quelle che presentano un legame evidente con essa, come i dati genetici[11].

Un'ulteriore interpretazione sposta il baricentro dell'analisi

dal contenuto del dato al contesto del trattamento, sostenendo che, nell'ambito sanitario, la qualificazione del dato dipende soprattutto dall'ambiente in cui esso viene utilizzato. In questa prospettiva, assumerebbero rilievo non solo i dati strettamente sanitari, ma anche quelli di natura amministrativa, in quanto spesso inscindibili nel corso delle attività svolte da professionisti e strutture sanitarie. Tale impostazione consente di graduare le informazioni in base al loro livello di sensibilità e risulta coerente con l'evoluzione dell'ordinamento.

Con l'entrata in vigore del Regolamento (UE) 2016/679, come detto in precedenza, il legislatore europeo ha però attribuito autonoma rilevanza alla nozione di dato relativo alla salute[12], ridefinendo il quadro complessivo e rafforzando le garanzie di tutela. In merito, l'art. 4, par. 1, n. 15 del Regolamento definisce i «*dati relativi alla salute*»[13] come «*i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*».

La scelta di sottoporre tali dati a una disciplina più stringente trova fondamento nella loro particolare capacità di incidere negativamente sulla vita privata dell'individuo, soprattutto in caso di utilizzi impropri o illeciti. Infatti, in ambito sanitario, il trattamento di dati appartenenti a categorie particolari avviene in modo sistematico e su larga scala, coinvolgendo strutture complesse e una pluralità di soggetti, circostanza che accresce il rischio di violazioni e impone un elevato livello di responsabilizzazione del titolare del trattamento.

Per tale motivazione esaminando il *Considerando* 51 viene specificato come dati personali in questo senso hanno bisogno di una protezione specifica, poiché sensibili[14] da un punto di vista dei diritti e delle libertà fondamentali.

Leggendo, a questo punto, il primo paragrafo dell'art. 9 del GDPR[15] si sancisce come principio di carattere generale il divieto di trattare dati personali, compreso quelli sanitari. Quest'ultimo, però, non vige in maniera assoluta, poiché all'interno del paragrafo 2 del medesimo articolo emergono una serie di condizioni per cui tali dati possono e/o devono essere trattati, facendo venire meno la preclusione[16]. In linea generale[17] sono due le categorie che consentono il trattamento dei dati. In primo luogo, in campo privatistico non opera la preclusione quando il trattamento risulti strettamente funzionale alla tutela della salute dell'individuo. In particolare, esso è consentito per finalità di prevenzione, medicina del lavoro, accertamento dell'idoneità lavorativa, nonché per attività di diagnosi, cura e assistenza sanitaria o sociale[18]. In secondo luogo, nella sfera pubblicistica il trattamento viene autorizzato quando ci sono motivi di interesse pubblico[19] in ambito sanitario[20].

Un trattamento che deve comunque essere ‹‹*proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*››[21]. Dalla norma in esame si ricava che, per i trattamenti di dati strettamente funzionali all'erogazione della prestazione sanitaria, il consenso dell'interessato non costituisce più un presupposto necessario di liceità[22]. Tale esonero opera indipendentemente dal contesto in cui il professionista sanitario svolge la propria attività, trovando applicazione sia nell'ambito delle strutture sanitarie pubbliche sia nell'esercizio della professione in forma privata o autonoma[23]. Ne consegue che il consenso dell'interessato continua a rappresentare un presupposto necessario in relazione a specifiche tipologie di trattamento.

Ciò avviene, in particolare, con riferimento all'utilizzo di applicazioni digitali in ambito sanitario, quando la raccolta dei dati personali avvenga per finalità ulteriori e diverse rispetto alla telemedicina. Analoga esigenza si riscontra nei trattamenti effettuati mediante il Fascicolo Sanitario Elettronico[24], per i quali la normativa di settore richiede espressamente l'acquisizione del consenso quale condizione di liceità, come confermato dal rinvio operato dal Codice della privacy alle relative disposizioni speciali[25].

Dunque, proprio in considerazione di tali potenziali impatti, il trattamento dei dati sanitari è generalmente qualificato come attività ad alto rischio, richiedendo l'adozione di misure tecniche e organizzative adeguate e un'attenta valutazione preventiva delle conseguenze che il trattamento può produrre sugli interessati. Ciò perché in ambito sanitario, il trattamento dei dati non rappresenta un'attività accessoria, ma una componente strutturale dell'erogazione delle prestazioni, rendendo necessaria l'adozione di garanzie rafforzate e di modelli organizzativi adeguati. Inoltre, la centralità dei diritti della persona rappresenta il presupposto per l'elaborazione di un sistema di governance della sicurezza delle informazioni in ambito sanitario.

I sistemi di gestione come strumenti di conformità organizzativa

Assume un rilievo importante il ruolo che hanno i soggetti coinvolti nell'attività e nella gestione del trattamento dei dati, compreso quelli sanitari. Infatti, nel sistema delineato dal Codice della Privacy, il trattamento dei dati personali ruotava attorno a tre figure fondamentali[26]: il titolare[27], il responsabile e l'incaricato del trattamento.

Il titolare era individuato nel soggetto, persona fisica o giuridica, cui spettava il potere decisionale in ordine alle

finalità e alle modalità del trattamento, inclusi i profili relativi alla sicurezza dei dati. Accanto a tale figura operava il responsabile del trattamento, chiamato a svolgere le attività materiali di gestione dei dati sulla base delle istruzioni impartite dal titolare.

Il quadro viene completato dagli incaricati, ossia le persone fisiche autorizzate a compiere specifiche operazioni sui dati personali. Con l'entrata in vigore del Regolamento (UE) 2016/679[28], la distinzione tra titolare e responsabile viene confermata, ma inserita in un contesto profondamente rinnovato. Il GDPR introduce, infatti, il principio di responsabilizzazione e amplia il perimetro soggettivo della gestione dei dati, prevedendo anche la figura della contitolarità del trattamento.

Tale ipotesi ricorre quando due o più soggetti determinano congiuntamente finalità e mezzi del trattamento, rendendo necessario un coordinamento strutturato tra le parti. In presenza di contitolari[29], il Regolamento impone la definizione di accordi interni che disciplinino in modo trasparente la ripartizione delle responsabilità, le modalità di esercizio dei diritti degli interessati e i punti di contatto con questi ultimi.

Resta, tuttavia, ferma la responsabilità individuale di ciascun contitolare nei confronti della normativa europea e del sistema sanzionatorio previsto. Diversamente dal Codice della Privacy, il GDPR non contempla espressamente la figura autonoma dell'incaricato del trattamento. Ciò nonostante, tale figura non risulta incompatibile con l'impianto del Regolamento. Sul punto, il Garante per la protezione dei dati personali ha chiarito la possibilità di individuare soggetti specifici, operanti sotto l'autorità del titolare o del responsabile, incaricati di svolgere compiti determinati mediante apposite designazioni scritte. Questa prassi, pur non obbligatoria, contribuisce a rafforzare la tracciabilità delle

responsabilità e la dimostrabilità della conformità.

In tale prospettiva, la gestione dei ruoli e delle responsabilità si inserisce in un modello più ampio di governance del trattamento dei dati, nel quale la documentazione assume un valore centrale quale strumento di accountability. La documentazione assume un ruolo centrale con l'entrata in vigore del GDPR. Diversamente dal passato, dove il Codice della Privacy richiedeva il documento programmatico sulla sicurezza (DPS), oggi è obbligatorio registrare tutte le attività di trattamento, anche mediante appositi registri che consentono di dimostrare la conformità normativa.

Tali registri includono informazioni sul titolare, sul responsabile, sulle categorie di dati e interessati, sulle finalità del trattamento, sui destinatari dei dati e sulle misure di sicurezza adottate. Essi sostituiscono in larga misura le vecchie notificazioni al Garante, ormai superate dal nuovo approccio europeo basato sulla responsabilizzazione e sulla documentazione interna.

Il Regolamento (UE) 2016/679 attribuisce un ruolo centrale alla protezione e alla sicurezza dei dati personali, imponendo ai titolari e ai responsabili del trattamento l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato ai rischi connessi alle attività di trattamento. In particolare, l'articolo 32 del GDPR[30] richiede che tali misure siano idonee ad assicurare la riservatezza, l'integrità e la disponibilità dei dati, considerando lo stato dell'arte, dei costi di attuazione, della natura dei dati trattati e delle possibili conseguenze per i diritti e le libertà delle persone fisiche.

Tra le misure espressamente richiamate dal regolamento rientrano la cifratura dei dati personali, la capacità di garantire la continuità dei servizi e di ripristinare tempestivamente l'accesso ai dati in caso di incidenti di natura tecnica o fisica, nonché l'adozione di procedure volte

a testare e verificare periodicamente l'efficacia delle misure di sicurezza implementate. Tali previsioni evidenziano come la sicurezza del trattamento non debba essere intesa come un risultato statico, bensì come un processo dinamico, fondato su un continuo monitoraggio e aggiornamento delle misure adottate.

Il Regolamento disciplina, inoltre, in modo puntuale la gestione delle violazioni dei dati personali, imponendo specifici obblighi di comunicazione in caso di *data breach*[31]. Infatti, qualora si verifichi un incidente che comporti la distruzione, la perdita, la modifica o la divulgazione non autorizzata di dati personali[32], il titolare del trattamento è tenuto a notificare l'evento all'autorità di controllo competente entro settantadue ore dal momento in cui ne è venuto a conoscenza[33]. Nei casi in cui la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati, è inoltre previsto l'obbligo di informare direttamente questi ultimi, al fine di consentire loro di adottare eventuali misure di tutela.

Un ruolo fondamentale in tale prospettiva è svolto dall'articolo 25 del GDPR[34], che introduce i principi di *privacy by design*[35] e *privacy by default*[36]. Secondo tali principi, i servizi, i prodotti e i processi che comportano il trattamento di dati personali devono essere progettati sin dalle fasi iniziali in modo da garantire un elevato livello di protezione delle informazioni. La tutela della *privacy*, pertanto, non può essere considerata un elemento aggiuntivo o successivo, ma deve essere incorporata strutturalmente nella progettazione e nell'implementazione dei sistemi. Entrando nello specifico, il principio di *privacy by design*, si fonda su un approccio preventivo alla protezione dei dati, volto ad anticipare e ridurre i rischi prima che si traducano in violazioni concrete.

Ciò implica che la sicurezza debba accompagnare l'intero ciclo di vita del dato: dalla raccolta fino alla cancellazione. Questo per garantire trasparenza nei processi, tracciabilità delle operazioni e rispetto costante dei diritti dell'interessato. Parallelamente, il principio di *privacy by default* richiede che, in assenza di scelte espresse dall'utente, siano applicate automaticamente le impostazioni più restrittive in termini di trattamento dei dati, limitando la raccolta e l'utilizzo delle informazioni a quanto strettamente necessario.

Sicurezza informatica in sanità e modelli di governance dei dati

In questo contesto, accanto alle previsioni normative del GDPR, assumono rilievo alcuni *framework* operativi elaborati a livello internazionale, finalizzati a supportare le organizzazioni nell'implementazione concreta delle misure di sicurezza.

Tra questi, particolare importanza rivestono i *Critical Security Controls* del C.I.S.[37], che offrono un insieme strutturato di controlli tecnici e organizzativi orientati alla prevenzione e alla mitigazione dei principali rischi informatici. In particolare, i *CIS Critical Security Controls* costituiscono un *framework* articolato di misure prioritarie, sviluppato per contrastare le minacce informatiche più ricorrenti e rilevanti.

Essi si fondano su un approccio pragmatico e basato sul rischio, individuando una serie di controlli considerati essenziali per rafforzare il livello di sicurezza dei sistemi informativi e dei dati trattati. La struttura dei controlli consente alle organizzazioni di adottare misure proporzionate alle proprie dimensioni, alla complessità operativa e al contesto di rischio, favorendo un'implementazione graduale ed

efficace delle politiche di sicurezza. I *CIS Critical Security Controls* sono suddivisi in differenti aree di intervento, che comprendono, tra le altre, la gestione e l'inventario degli asset informatici, la protezione dei dati, il controllo degli accessi, la gestione delle vulnerabilità e la risposta agli incidenti di sicurezza.

Tale segmentazione consente di affrontare in modo sistematico le principali superfici di attacco, riducendo il rischio di accessi non autorizzati, perdite di dati e interruzioni dei servizi essenziali. Sotto il profilo della conformità normativa rappresentano uno strumento di supporto concreto all'adempimento degli obblighi previsti dal GDPR, in particolare di quelli relativi alla sicurezza del trattamento e alla responsabilizzazione del titolare e del responsabile.

L'adozione di controlli tecnici e organizzativi strutturati agevola, infatti, la dimostrabilità della conformità alle prescrizioni dell'articolo 32 del Regolamento, nonché l'attuazione dei principi di *privacy by design* e *privacy by default*. Inoltre, l'utilizzo dei *CIS Critical Security Controls* favorisce una maggiore capacità dell'organizzazione di prevenire e gestire eventi di sicurezza, contribuendo a ridurre la probabilità e l'impatto delle violazioni dei dati personali. In tale prospettiva, il *framework* si inserisce in un modello di sicurezza dinamico, fondato sul monitoraggio continuo, sull'aggiornamento delle misure adottate e sulla consapevolezza del personale coinvolto nei processi di trattamento.

Sebbene i *CIS Critical Security Controls* rappresentino uno strumento operativo particolarmente efficace per l'implementazione concreta delle misure di sicurezza, essi non si configurano come uno standard certificabile, né come un sistema di gestione strutturato. Per tale ragione, al fine di garantire un approccio organico, sistematico e orientato al miglioramento continuo della sicurezza delle informazioni, assume rilievo l'adozione di modelli di *governance* più

articolati, tra cui la ISO/IEC 27001:2022[38].

La ISO/IEC 27001[39] si inserisce come cornice organizzativa di riferimento per la gestione della sicurezza delle informazioni, consentendo di integrare i controlli tecnici e operativi, quali quelli previsti dai *CIS Critical Security Controls*, all'interno di un sistema di gestione strutturato. Mentre quest'ultimi offrono indicazioni concrete sulle misure da adottare, la ISO/IEC 27001 fornisce il metodo per governare tali misure in modo coerente con gli obiettivi strategici dell'organizzazione, con il contesto operativo e con i requisiti normativi applicabili.

Il Sistema di Gestione della Sicurezza delle Informazioni, disciplinato dallo standard internazionale ISO/IEC 27001 nella versione aggiornata del 2022, si configura come un presidio organizzativo essenziale per assicurare il rispetto degli obblighi normativi e una gestione ordinata dei rischi connessi alle informazioni. La norma individua i requisiti necessari per progettare, implementare, mantenere e migliorare in modo continuo un sistema orientato alla protezione della riservatezza, dell'integrità e della disponibilità delle informazioni, adottando un metodo strutturato fondato sull'analisi e sul trattamento del rischio.

L'implementazione di un *ISMS* rappresenta una decisione di carattere strategico, strettamente legata agli obiettivi dell'organizzazione, al contesto in cui essa opera e alle aspettative delle parti interessate. In tale ottica, la sicurezza delle informazioni non viene ridotta a una funzione tecnica isolata, ma assume una dimensione trasversale, integrata nei processi decisionali e nei meccanismi di governo dell'ente.

La ISO/IEC 27001 richiede, infatti, che il sistema di gestione sia coerente con la struttura organizzativa e adeguato alle caratteristiche, alle dimensioni e al livello di complessità dell'organizzazione. Un profilo di particolare rilievo

dell'*ISMS* è rappresentato dalla sua funzione di supporto alla conformità giuridica, regolamentare e contrattuale, inclusi gli obblighi in materia di protezione dei dati personali e sicurezza informatica. Attraverso attività sistematiche di valutazione e trattamento del rischio, l'organizzazione è tenuta a identificare le minacce rilevanti e a individuare misure di sicurezza appropriate, anche mediante il riferimento ai controlli previsti dall'Allegato A[40], che offre una cornice ordinata delle possibili misure di protezione[41].

Lo standard ISO/IEC 27001, successivamente, riconosce un ruolo determinante alla *leadership*[42], attribuendo all'alta direzione la responsabilità primaria del funzionamento e dell'efficacia del sistema di gestione della sicurezza delle informazioni. In particolare, il vertice aziendale è chiamato a garantire un impegno concreto, assicurando che la politica e gli obiettivi di sicurezza siano coerenti con l'indirizzo strategico dell'organizzazione e pienamente integrati nei processi operativi. La politica per la sicurezza delle informazioni costituisce il fondamento dell'*ISMS*, poiché definisce i principi generali, gli impegni dell'organizzazione e il quadro di riferimento per la determinazione degli obiettivi di sicurezza. Essa deve risultare adeguata allo scopo dell'ente, prevedere il rispetto dei requisiti applicabili e promuovere il miglioramento continuo del sistema.

La sua formalizzazione e diffusione contribuiscono a rafforzare la cultura organizzativa della sicurezza e a incrementare la consapevolezza del personale in merito ai comportamenti richiesti e alle conseguenze derivanti da eventuali violazioni. Accanto al ruolo della leadership, assume rilievo centrale la chiara definizione delle responsabilità e delle autorità in materia di sicurezza delle informazioni.

La norma impone che i ruoli chiave siano formalmente individuati e comunicati, assicurando la presenza di soggetti

incaricati della conformità dell'*ISMS* e della valutazione delle sue prestazioni. Un'adeguata strutturazione delle responsabilità consente di evitare frammentazioni organizzative e favorisce un coordinamento efficace tra le diverse funzioni aziendali coinvolte. Inoltre, un elemento distintivo della ISO/IEC 27001:2022 è rappresentato dalla sua integrazione nei sistemi di *governance* dell'organizzazione.

L'adozione di una struttura di alto livello, comune ad altri standard sui sistemi di gestione, agevola l'approccio integrato alla conformità, consentendo di coordinare la sicurezza delle informazioni con ulteriori ambiti organizzativi, quali la gestione della qualità, la continuità operativa e il risk management. In questo contesto, l'*ISMS* si configura come uno strumento di governo, in grado di collegare gli obblighi normativi ai processi decisionali e ai meccanismi di controllo interno.

Le attività di monitoraggio[43], gli *audit* interni[44] e il riesame periodico[45] da parte della direzione permettono di verificare costantemente l'efficacia del sistema e di individuare tempestivamente eventuali non conformità, nonché possibili margini di miglioramento. La compliance, pertanto, non è più concepita come un adempimento statico e formale, ma come un processo continuo e dinamico, inserito nella strategia complessiva dell'organizzazione.

Il sistema di gestione della sicurezza delle informazioni contribuisce così a rafforzare l'affidabilità dell'ente, la fiducia delle parti interessate e la capacità di prevenire e gestire i rischi, affermandosi come uno strumento essenziale di conformità organizzativa e di corretta *governance*.

In conclusione, l'analisi ha evidenziato come la sicurezza informatica in sanità rappresenti oggi un elemento essenziale per garantire la conformità al GDPR e la protezione dei dati sanitari, richiedendo l'integrazione tra strumenti normativi,

organizzativi e standard internazionali di sicurezza delle informazioni. La gestione del rischio emerge come asse portante della governance digitale, in grado di connettere obblighi giuridici e misure tecniche in un approccio sistemico e strutturato.

Nel successivo articolo verrà analizzato il tema della gestione del rischio informatico, con particolare riferimento alla DPIA (Data Protection Impact Assessment), alla ISO/IEC 27005 e all'approccio sistematico alla valutazione e mitigazione del rischio nelle organizzazioni sanitarie.

Per approfondire ulteriormente il tema, è possibile scaricare il white paper gratuito a cura di **Piergiorgio Verrecchia**, dal titolo **"La gestione del rischio informatico in ambito sanitario come misura tecnico-organizzativa di conformità normativa",** che fornisce un'analisi operativa e applicativa dei modelli di risk management in ambito sanitario.

Note

[1] A. ZUCCHETTI, *Dati (trattamento dei)*, in. V. ITALIA (a cura di), *Enciclopedia degli Enti Locali, Atti, Procedimenti, Documentazione*, Giuffrè, Milano, 2007, p. 811.

[2] D.U. GALETTA*, Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *Federalismi.it,* 5, 2016, p. 9.

[3] Il Regolamento del Parlamento europeo e del Consiglio dell'Unione europea abroga la precedente Direttiva 95/46/CE.

[4] Ratificata nell'ordinamento italiano con legge 21 febbraio 1989, n. 98 *‹‹Ratifica ed esecuzione della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981››.*

[5] Si veda l'art. 8, par. 1 che recita: *«Gli Stati membri*

vietano il trattamento dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento dei dati relativi alla salute e alla vita sessuale».

[6] G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi,* Bologna, 2012, p. 57-61; E. VARANI, *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario: dalla Carta dei diritti fondamentali dell'Unione europea al d.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"*, in Giur.it, 2005, p. 1769.

[7] Tale assunto è condiviso da P. GUARDA*, I dati sanitari*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, p. 594.

[8] F. CAGGIA, *Il trattamento dei dati dei dati sanitari sulla salute, con particolare riferimento all'ambito sanitario*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, p. 407-410.

[9] G. FINOCCHIARO, op. cit., p. 62-63.

[10] Raccomandazione (97) 5 del Comitato dei Ministri agli Stati membri relativa alla protezione dei dati sanitari, adottata dal Comitato dei Ministri il 13 febbraio 1997.

[11] Si rinviene traccia dell'applicazione nazionale di tale disposizione negli artt. 22 e 23 della legge.

[12] Si veda di nuovo: art. 4, par. 1 del Regolamento 2016/679/UE.

[13] Il Considerando 35 si riferisce ad ogni informazione utile dell'interessato oltre che presente, anche passata e futura, ridefinendo così la sua portata normativa.

[14] Anche se la Cassazione cataloga i dati riguardi la salute ed il sesso come “super sensibili” poiché toccano la persona in senso stretto e perciò bisognosi di una protezione maggiore rispetto agli altri dati. Si veda in merito Cass. civ., sez. VI, 2016, n. 222.

[15] Art. 9 GDPR, par. 1: “È *vietato trattare dati personali che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona*”.

[16] Il legislatore europeo ha confermato la precedente impostazione. Infatti, l’art. 8, par. 2 della previgente Direttiva 95/46/CE prevedeva alcune deroghe al divieto del trattamento dei dati particolarmente sensibili, tra cui quelli sanitari.

[17] Si veda per completezza art. 9, par. 2.

[18] Art. 9, par. 2, lett. h.

[19] Il considerando 52 del Regolamento chiarisce che la deroga al divieto di trattamento dei dati particolari può trovare applicazione in presenza di esigenze legate alla tutela della salute, comprendendo tanto la sanità pubblica quanto l’organizzazione e la gestione dei servizi di assistenza sanitaria. In tale prospettiva, il trattamento è funzionale anche a garantire l’efficienza e la sostenibilità delle procedure connesse all’erogazione delle prestazioni sanitarie e assicurative, nonché allo svolgimento di attività di archiviazione nel pubblico interesse, di ricerca scientifica o storica e di analisi statistica. La medesima deroga, inoltre, legittima il trattamento dei dati qualora esso risulti necessario per l’accertamento, l’esercizio o la difesa di diritti in ambito giudiziario, amministrativo o

stragiudiziale.

[20] Art. 9, par. 2, lett. i.

[21] Art. 9, par. 2, lett. g.

[22] Seppur la lettera a dell'art. 9 parla di consenso e soprattutto che il trattamento si effettua quando l'interessato abbia espresso un consenso esplicito per finalità determinate, fatta salva l'ipotesi in cui il diritto dell'Unione o quello nazionale escludano la possibilità di rimuovere il divieto previsto.

[23] M. L. RIZZO*, La disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, in M. IASELLI (a cura di), *La tutela dei dati personali in ambito sanitario*, Giuffrè Francis Lefebvre, Milano, 2020, p. 7-8.

[24] Il FSE è *«l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito»,* ai sensi dell'art. 12, comma 1, del decreto-legge 18 ottobre 2012, n. 179 (convertito con modificazioni dalla legge 17 dicembre 2012, n. 221.

[25] Il decreto-legge 19 maggio 2020, n. 34, noto come *"Decreto Rilancio"*, ha inciso sulla disciplina del fascicolo sanitario elettronico, escludendo la necessità del consenso dell'interessato per le operazioni di alimentazione dello stesso. Resta invece fermo l'obbligo di acquisire il consenso per la consultazione del Fascicolo da parte dei professionisti sanitari abilitati.

[26] D.lgs. 196/2003, aggiornato dal D.lgs. 101/2018: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale

sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018). Si veda per una maggiore visione: *www.gazzettaufficiale.it.*

[27] Il ruolo affidato a tale soggetto era già noto nella vigenza della Direttiva 95/46/CE, nonché della L. 675/1996 inerente alla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. L'art. 1, lett. d) della citata legge sanciva che per titolare del trattamento si intende «*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali, ivi compreso il profilo della sicurezza*»

[28] Si rinvia anche al Regolamento UE/2018/1725 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE; *European Data Protection Supervisor, EDPS Guidelines on the concept of controller, processor and joint controllership under Regulation* (EU) 2018/1725.

[29] Secondo cui «*allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*››.

[30] Art. 32 GDPR, par. 1, enuncia ‹‹ *Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*››.

[31] Art. 33 GDPR sancisce: ‹‹*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*››.

[32] Linee Guida EDPB n. 1/2021 espone 6 regole da seguire in caso di data breach: segnalare, identificare, valutare, notificare, comunicare, registrare e apprendere.

[33] *L'European Data Protection Board* ha adottato in data 28-03-2023, dopo una fase di consultazione pubblica partita a settembre 2022 (09/2022), la versione 2.0 delle linee guida riguardanti gli obblighi di notifica delle violazioni dei dati personali.

[34] Art. 25 GDPR, par. 1, enuncia ‹‹*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*››;

par. 2:‹‹ *Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*››.

[35] Protezione dei dati personali venga garantita fin dalla progettazione.

[36] Protezione dei dati personali sia garantita per impostazione predefinita.

[37] *Center for Internet Security* in *www.cisecurity.org.*

[38] In questo contesto dobbiamo fare riferimento alla NIS 2 che pur non prevedendo espressamente l'obbligo di adottare specifici standard tecnici, la Direttiva incoraggia l'impiego di *framework* riconosciuti a livello internazionale al fine di

assicurare un adeguato livello di protezione delle reti e dei sistemi informativi. In questa prospettiva, lo *standard* ISO/IEC 27001 costituisce uno dei principali riferimenti metodologici per l'implementazione operativa delle misure di gestione del rischio previste dal quadro normativo europeo. *Lo standard* si basa su un approccio strutturato alla sicurezza delle informazioni, fondato sul modello di miglioramento continuo *Plan-Do-Check-Act* (PDCA).

Attraverso tale schema metodologico, le organizzazioni sono chiamate a individuare i propri asset informativi, analizzare i rischi connessi alla loro gestione e implementare misure di sicurezza adeguate volte a mitigare tali rischi e a mantenerli entro livelli considerati accettabili. Questo modello di gestione del rischio risulta pienamente in linea con l'impostazione adottata dalla Direttiva NIS 2, la quale richiede alle entità interessate l'adozione di politiche organizzative e procedure strutturate finalizzate alla prevenzione, al monitoraggio e alla gestione degli incidenti di sicurezza informatica.

Le sinergie tra la Direttiva NIS 2 e lo *standard* ISO/IEC 27001 si manifestano in particolare con riferimento a diversi elementi centrali della governance della sicurezza informatica. Tra i principali aspetti di convergenza è possibile individuare: la definizione di politiche organizzative per la sicurezza delle informazioni; l'adozione di metodologie strutturate per l'analisi e il trattamento del rischio; l'implementazione di controlli tecnici e organizzativi finalizzati alla protezione delle infrastrutture informatiche; la predisposizione di procedure per la gestione degli incidenti di sicurezza e delle vulnerabilità; la promozione di attività di formazione e sensibilizzazione del personale sui temi della cybersecurity.

L'implementazione di un sistema di gestione conforme allo *standard* ISO/IEC 27001 consente pertanto alle organizzazioni di strutturare in modo sistematico e coerente le proprie

politiche di sicurezza informatica, contribuendo al contempo a facilitare l'adempimento degli obblighi previsti dalla Direttiva NIS 2. In questa prospettiva, lo *standard* può essere considerato uno strumento operativo di particolare rilevanza, in quanto permette di tradurre i principi generali stabiliti dalla normativa europea in procedure organizzative concrete e applicabili all'interno dei contesti aziendali.

[39] ‹‹*ISO (International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization*››.

[40] *Table* A.1 *information security controls reference*, ISO/IEC 27001: 2022, p. 11.

[41] Si veda l'Appendice A alla fine del presente elaborato, pp.69-71.

[42] ISO/IEC 27001: *Top management shall demonstrate leadership and commitment with respect to the information security management system by:*

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

[43] ISO/IEC 27001: ‹‹*The organization shall determine: a) what needs to be monitored and measured, including information security processes and controls; b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid; c) when the monitoring and measuring shall be performed; d) who shall monitor and measure; e) when the results from monitoring and measurement shall be analysed and evaluated; f) who shall analyse and evaluate these results. Documented information shall be available as evidence of the results. The organization shall evaluate the information security performance and the effectiveness of the information security management system*››, p.8.

[44] ISO IEC 27001: ‹‹*The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organization's own requirements for its information security management system; 2) the requirements of this document; b) is effectively implemented and maintained*››.

[45] ISO IEC 27001: ‹‹*The management review shall include consideration of: a) the status of actions from previous management reviews; b) changes in external and internal issues that are relevant to the information security management system; c) changes in needs and expectations of interested parties that are relevant to the information security management system; d) feedback on the information security*

performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; 4) fulfilment of information security objectives; e) feedback from interested parties; f) results of risk assessment and status of risk treatment plan; g) opportunities for continual improvement››.

Profilo Autore

Praticante avvocato con una formazione avanzata all'intersezione tra diritto e innovazione tecnologica. Laureato in Giurisprudenza presso l'Università degli Studi del Molise, ha successivamente conseguito un Master di II livello in Informatica Giuridica, Nuove Tecnologie e Diritto dell'Informatica presso l'Università La Sapienza di Roma, con una ricerca focalizzata sulla gestione del rischio informatico in ambito sanitario come misura tecnico-organizzativa di conformità normativa.
Il suo ambito di interesse e approfondimento comprende la cybersecurity compliance, la protezione dei dati personali, la responsabilità giuridica legata all'uso delle tecnologie digitali e le implicazioni normative dei sistemi informatici in settori ad alta criticità.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/sicurezza-informatica-in-sanita/