Il trattamento dei dati sanitari

Questo articolo fa parte della serie legata al tema della cybercriminalità nel settore sanitario, un percorso di analisi che intreccia sanità digitale, protezione dei dati e sicurezza informatica. L'attenzione si concentra sul concetto di dati sanitari, considerati il nucleo più sensibile della privacy. Essi, infatti, non solo riflettono la condizione clinica di un individuo, ma ne svelano la dimensione più intima, richiedendo tutele rafforzate sia sul piano normativo che tecnologico.

Così la Dr.ssa Salvadori Angelica, consigliere dell'Ordine dei Medici Chirurghi e Odontoiatri della Provincia di Torino:

> *"La prima cosa che faccio quando arrivo in studio è accendere il computer. E con questo gesto apro, in qualche modo inconsapevole, una finestra, anzi una porta attraverso la quale, nel corso della giornata, i dati dei miei pazienti potranno essere disseminati in molte direzioni. […] Ad esempio, mi metto in collegamento con il SAR (Sistema di Accoglienza Regionale) della Regione Piemonte e il SAC (Sistema di Accoglienza Centrale) quando compilo in modalità informatica una ricetta dematerializzata contenente prescrizioni farmaceutiche e specialistiche, mi collego con AURA (Archivio Unico Regionale degli Assistiti della Regione Piemonte) se emerge l'esigenza di un aggiornamento dell'anagrafe degli assistiti, mi connetto con l'INPS (Istituto Nazionale della Previdenza Sociale) quando rilascio un certificato di malattia, oppure con l'INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro) se devo certificare un infortunio lavorativo, con il CSI Piemonte (Consorzio per il Sistema Informativo) se devo vedere l'esito di un tampone per Covid 19, se devo richiederne uno, se devo verificare l'inizio o la fine di una quarantena o di un isolamento, se devo vedere se un paziente*

è vaccinato. E questo vale non solo per me, medico di medicina generale, ma per tutti i medici convenzionati con il SSN, per i medici specialisti ospedalieri e, per alcuni aspetti, anche per i medici liberi professionisti.Se i medici, forse, non sempre sono consapevoli di tutto quello che mettono in moto, viene da chiedersi: e i cittadini? Hanno una percezione corretta di tutte le strade che possono prendere i loro dati sanitari?”.[1]

Nel discorrere del primo capitolo si è potuto constatare come, grazie alle potenzialità offerte dall’innovazione tecnologica, i dati sanitari stiano acquisendo sempre maggior impiego nel mondo contemporaneo: dalla ricerca medica e farmaceutica alla gestione dei servizi sanitari pubblici e privati.[2]

La materia inerente alla protezione dei dati sanitari è stata definita “diritto inquieto”[3], vi è difatti una tensione che caratterizza i dati sanitari stessi: meritevoli da un lato di massima protezione e riservatezza, e dall’altro di una calibrata circolazione per esigenze di sanità pubblica (si pensi alla destinazione ai fini di ricerca). A tale poi già complesso bilanciamento si aggiunge il problema della sicurezza rispetto a possibili attacchi informatici che possono mettere a rischio tanto la privacy degli individui quanto la tutela della salute pubblica.

Occorrerà comunque dapprima inquadrare ontologicamente le categoria dei dati idonei a rivelare lo stato di salute.

Alquanto nota è difatti la formula che consente di qualificare i dati sanitari come “nocciolo (o nucleo) duro” della privacy, locuzione utilizzata da chi rileva come essi si collochino “nel cerchio concentrico più interno” o, se si vuole, all’estremo più elevato della “scala delle durezze”[4] della protezione dei dati personali, risultando invero capaci di far intravedere, quando non di svelare del tutto, la sfera più riservata della persona.[5]

Ed è proprio dalla loro alta sensibilità che si ricava la necessità di una maggior tutela nel trattamento rispetto a quello indirizzato ad altre tipologie di dati, in quanto, se non correttamente svolto, potrebbe ingenerare rischi significativi per il rispetto dei diritti e delle libertà fondamentali dell'individuo, esponendo quest'ultimo a potenziali discriminazioni, stigmatizzazioni e classificazioni.

Il quadro normativo di riferimento è sicuramente esteso, ad ogni modo come fonti principali si possono indicare il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio per come relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, anche meglio noto come GDPR (*General Data Protection Regulation*), che abroga la direttiva 95/46/CE;[6] a cui si aggiunga il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, conosciuto anche come Codice della privacy), aggiornato ed integrato con le modifiche introdotte dal decreto legislativo del 10 agosto 2018, n. 101, quale recante disposizioni per l'adeguamento della normativa nazionale al regolamento (UE) anzidetto. [7]

Prima di affrontare la spinosa questione della protezione dei dati personali si vogliono fissare alcune preliminari definizioni, guardando innanzitutto alle disposizioni del Regolamento 2016/679/UE.

L'art. 4, par. 1, n. 1 del testo normativo sopradetto infatti chiarisce come per dato personale si debba intendere: "*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 ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica,*

fisiologica, genetica, psichica, economica, culturale o sociale".

Entro l'ampia categoria dei dati personali si rinviene poi il sottoinsieme dei cosiddetti "dati particolari" (ex dati sensibili, nel vecchio codice privacy), definiti dall'art. 9 del GDPR come: "*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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*".

Si noti come i dati relativi alla salute figurino proprio fra i dati particolari, cioè quei dati la cui conoscenza da parte di altri può recare un grave pregiudizio per l'interessato.

Addentrandosi ancora più nel dettaglio della normativa il *Considerando* 35 del GDPR puntualizza come fra i dati inerenti alla salute dovrebbero rientrare :

> *"tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. […] Le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro".*

Si comprende allora il motivo per cui i dati sanitari, ipersensibili, espressivi della più autentica essenza della privatezza, siano proprio quella tipologia di dati ad andare a beneficiare di una maggior tutela accordata dall'ordinamento,

per come espressa in: misure di garanzia rafforzate, presupposti di liceità del trattamento particolarmente stringenti, stretta indispensabilità a fini informativi, divieto di divulgazione, e si intuirà altresì la ragione per cui siano necessitanti di una protezione rafforzata rispetto a tutti quei rischi di intrusione ed accesso indebito, alterazione e manipolazione connessi a possibili attacchi cibernetici indirizzabili ai sistemi informativi sanitari.[8]

Principi cardine sulla protezione dei dati sanitari

Appurato come in ambito medico, ossia in qualsiasi struttura ospedaliera, RSA, ambulatorio del medico di base o del libero professionista, ad esser trattati sistematicamente siano soprattutto dati "particolari", si volgerà ivi lo sguardo alle disposizioni che vanno a disciplinarne le specifiche modalità di trattamento.

Preliminarmente tuttavia si passeranno in rassegna i sei principi generali, in tema di trattamento dei dati personali, elencati all'art. 5 del GDPR, quali presupposti fondamentali attorno a cui orbitano tutti i meccanismi di protezione dei dati.

In primis si annoveri il principio definito di liceità, correttezza e trasparenza (*lawfulness, fairness and transparency), in nome del quale si richiede che i dati "vengano trattati in modo lecito, corretto e trasparente nei confronti degli interessati*", ciò implica dunque che qualsiasi informazione ad essi inerente sia accessibile e di facile comprensione, grazie all'utilizzo di un linguaggio chiaro e semplice, nonché che gli interessati abbiano contezza dell'identità dei titolari del trattamento (ossia dei soggetti che per l'appunto trattano i dati personali) e delle finalità del trattamento stesso.

Calando tale principio nel panorama sanitario si può richiamare quanto previsto dall'Accordo Stato-Regioni sulla telemedicina del 17 dicembre 2020, il quale prevede specifici oneri informativi nei confronti dei pazienti soggetti a servizi di telemedicina fra cui: una completa descrizione della gestione dei dati, dei diritti dell'assistito, delle modalità di contatto, nonché un elenco aggiornato dei responsabili del trattamento.[9]

Il secondo principio invece è relativo alla limitazione delle finalità (*purpose limitation) dei dati, si rilevi come questi siano "raccolti per finalità determinate, esplicite e legittime",* per cui non sarà consentito trattarli successivamente in modo non compatibile con le finalità previamente delineate. Si tenga comunque presente che eventuali ulteriori trattamenti per finalità di pubblico interesse, di ricerca scientifica, storica o a fini statistici non sono considerati incompatibili con le finalità iniziali e risultano pertanto consentiti.

Il terzo principio è la c.d. minimizzazione dei dati (*data minimisation), in ragione del quale questi ultimi dovranno essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati".*

L'accuratezza poi (*accuracy*) è il quarto principio ed implica la necessità di garantire che i dati personali siano adeguatamente accurati ed aggiornati, ove necessario, adottando tutte le misure ragionevoli necessarie per cancellarli o rettificarli tempestivamente qualora inesatti rispetto alle finalità per cui vengono trattati.

Il quinto principio suole indicare la c.d. limitazione della conservazione (*storage limitation*), per cui i dati saranno "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*". Una eventuale conservazione per periodi di tempo più lunghi sarà

consentita unicamente per finalità di interesse pubblico, di ricerca scientifica, storica o a fini statistici. Le politiche di *data retention,* previste specificatamente dal nostro ordinamento, disciplinano infatti numerosi e differenziati tempi di conservazione per quanto concerne la documentazione sanitaria: sarà pertanto compito *dell'operatore* sanitario (pubblico o privato) dover identificare la natura della documentazione e conseguentemente la normativa di riferimento applicabile.

Per esemplificare, l'iconografia radiologica conta ad oggi un periodo di archiviazione di dieci anni, viceversa le cartelle cliniche, gli esami di laboratorio, i referti vedono un obbligo di conservazione illimitato nel tempo, in quanto rappresentanti atto ufficiale, indispensabile a garantire la certezza del diritto, nonché quale preziosa fonte documentaria per le ricerche di carattere storico sanitario.[10]

Il sesto ed ultimo principio riguarda infine l'integrità e la riservatezza dei dati (*integrity and confidentiality), ciò implicherà che vengano adottate tutte le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, inclusa la protezione contro "trattamenti non autorizzati o illeciti, la perdita, la distruzione o il danno accidentale".*

A titolo esemplificativo, si richiami l'elencazione all'art 32 par.1 del GDPR relativamente alle misure che possono essere adottate ed implementate al fine di garantire la sicurezza dei digital data, fra cui:

1. La pseudonimizzazione dei dati personali, ovvero una metodologia che si pone l'obiettivo di "allontanare" il dato dalla persona, rendendone così complessa la stessa riferibilità (senza tuttavia romperne il legame, a cui mirano invece le tecniche di anonimizzazione);[11]
2. La cifratura dei dati, volta a rendere i dati personali

incomprensibili a chiunque non sia autorizzato ad accedervi tramite una apposita chiave di lettura idonea a decriptarne l'informazione;
3. La capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità ed altresì la resilienza dei sistemi e dei servizi di trattamento;
4. La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
5. L'*auditing*, espressione volta ad indicare una procedura atta a testare, verificare, e valutare regolarmente l'efficacia delle misure tecniche e organizzative concretamente adottate.[12]

Si badi bene, il legislatore non entra nel dettaglio, anzi quello fornito risulta pressoché un elenco generale, poiché è fondamentale che la security stessa venga garantita da soluzioni ritagliate nel modo più personale possibile rispetto alle specificità del soggetto da proteggere. Non pare essere dunque "codardia legislativa", ma diretta conseguenza dell'assunto secondo cui se il titolare del trattamento deve essere accountable allora dovrà parimenti essere libero di ritagliarsi il "vestito" di sicurezza che ritiene necessario per la propria struttura.

Il principio di accountability

Il medesimo art. 5 del GDPR, al secondo paragrafo, enuncia il principio di responsabilizzazione (o *accountability*), in assenza del quale i sei principi cardine previamente elencati non potrebbero esser attuati: sarà infatti precipua responsabilità del titolare del trattamento[13] predisporre e mettere in atto specifiche soluzioni tecniche e organizzative che rendano il trattamento lecito, corretto, trasparente, adeguato, limitato nel tempo, pertinente ed effettuato per finalità legittime; così come sarà sua stessa responsabilità risponderne e "render conto" dell'efficacia delle misure

concretamente impiegate e dei risultati così ottenuti.

Pertanto la figura apicale di una data struttura (si pensi ad un Direttore sanitario), tenuto conto della natura del dato, del suo ambito di applicazione (nell'erogazione di servizi di cura, in un progetto di ricerca *etc*.), del contesto (limitatamente alla propria struttura, od in condivisione con altre), delle finalità del trattamento, dei rischi per i diritti e le libertà delle persone fisiche, dovrà adottare misure tecniche ed organizzative adeguate, ossia parametrate al livello di rischio rilevato. Le anzidette misure poi, ex art. 24 GDPR, dovranno essere "*riesaminate ed aggiornate qualora necessario*", introducendo così il principio fondamentale della ciclicità della sicurezza, quale perimetro altamente dinamico da dover revisionare periodicamente nel tempo, al fine di ottenerne un sempre maggiore perfezionamento. [14]

Non vi è dubbio sul fatto che venga in tal modo a delinearsi un sistema di adeguamento al GDPR fortemente accentrato sulla figura del titolare del trattamento: data la riconosciuta difficoltà di esercizio dei diritti dell'interessato[15], essendo egli spesso propenso a rilasciare i propri dati con leggerezza o con carenza di consapevolezza, viene spostato il baricentro della responsabilità sul titolare del trattamento e sulla necessità che le operazioni di trattamento stesse siano "GDPR *compliant*".[16]

Ed è proprio così che il concetto di *accountability* si collega con quelli di prevenzione e proattività, inglobando il saper agire d'anticipo, pianificando, mediante policy e tecnologie efficaci, quanto necessario per evitare i rischi di compromissione dei dati. Fare ciò significa, ex art. 25 GDPR, operare una valutazione del rischio e del suo contenimento attraverso tecniche di protezione "fin dall'avvio del trattamento" (c.d. *privacy by default*) e "per impostazione predefinita" (c.d. *privacy by design*): tali espressioni puntualizzano come la privacy degli interessati dovrà essere

tutelata fin dall'inizio, cioè dalle fasi di ideazione e progettazione del servizio, e che non potranno esser trattati dati personali ulteriori rispetto a quelli minimi indispensabili per la specifica finalità del trattamento.[17]

Tali ragionamenti, per ciò che ivi più interessa, possono certo essere calati in ambito sanitario: i software, i dispositivi e le procedure utilizzati nella sanità digitale dovranno essere rispettosi della normativa in tema di protezione dei dati. Pertanto una corrispondenza di telemedicina fra medico e paziente con l'uso di sistemi non sicuri, come i *social* o la posta elettronica, costituisce di per sé una procedura a rischio, violante le regole sulla protezione dei dati, ed in quanto tale sanzionabile dall'Autorità Garante per la protezione dei dati.

Allora i sanitari, e le strutture che offrono servizi di telemedicina, hanno il precipuo dovere di gestire i rischi derivanti dal trattamento dei dati personali dei pazienti, optando per quelle soluzioni operative che offrano le migliori garanzie di proporzionalità, efficacia, sicurezza, e rispetto dei diritti della persona.[18]

Si voglia, già in questa sede, anticipare l'assoluto rilievo dell'innestare una cultura della (cyber)sicurezza mediante una adeguata formazione del personale medico, ed è così invero che recita l'articolo 32 comma 4 del GDPR: "*Il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare medesimo.*"

Si pensi ad una struttura sanitaria complessa (da un poliambulatorio ad un grande ospedale), in questa stessa gli operatori a trattare dati sanitari sono indubbiamente molteplici, ad ogni modo comunque tutti dovranno essere a conoscenza circa le procedure da seguire ed i conseguenti probabili rischi insiti nel trattamento di dati sensibili, in

particolar modo alla luce delle sempre più frequenti compromissioni degli archivi e sistemi digitali sanitari.

Il Data Protection Officer

Anche la designazione di un Responsabile della protezione dati (da qui in avanti indicato come DPO, acronimo inglese per *Data Protection Officer*) rientra nell'approccio responsabilizzante delineato dal GDPR, in linea col principio di *accountability.*

Tale figura professionale, designata dal titolare o dal responsabile[19] del trattamento, si presenta quale un consulente esperto, dotato di un'approfondita conoscenza della normativa e delle prassi in tema di gestione dei dati personali, nonché dello specifico settore di riferimento in cui si trova ad operare.

La nomina del DPO si presenta come obbligatoria, ex art. 37 del GDPR, ogniqualvolta il trattamento sia effettuato da una autorità pubblica o da un organismo pubblico, nonché quando le attività principali del titolare o del responsabile del trattamento consistano nel trattare, su larga scala, categorie particolari di dati personali (quali per l'appunto sono i dati inerenti alla salute).

Questo non significa che ogni medico sia obbligato a designare un DPO: il singolo professionista o il medico di base non trattano dati "su vasta scala", diversamente il problema si pone per gli studi in cui operano più medici e così anche per una Azienda sanitaria, un ospedale privato, una residenza sanitaria assistenziale, tutti si doteranno di tale figura dotata di competenze giuridiche, informatiche, nonché di *risk management*, la cui responsabilità sarà quella di osservare, valutare ed organizzare la gestione del trattamento dei dati personali (e dunque la loro protezione), affinché questi ultimi siano trattati nel rispetto delle normative privacy europee e nazionali.

L’art. 39 del GDPR opera poi una dettagliata elencazione delle principali funzioni del DPO, fra cui:

1. Informare e fornire una consulenza al titolare o al responsabile del trattamento in merito agli obblighi derivanti del Regolamento europeo;
2. Sorvegliare l’attuazione del Regolamento europeo, come anche vigilare sull’applicazione delle politiche del titolare del trattamento in materia di protezione dei dati personali, comprese l’attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti;
3. Fornire, se richiesto, un parere in merito alla valutazione d’impatto sulla protezione dei dati e sorvegliarne il concreto svolgimento. Essendo la valutazione d’impatto un processo volto a valutare la necessità e proporzionalità di un determinato trattamento e a gestirne gli eventuali rischi, il titolare del trattamento si consulterà preventivamente col DPO su tematiche quali: condurre o meno la valutazione stessa, quale specifica metodologia sia da adottare, quali salvaguardie e misure di sicurezza siano da applicare al fine di attenuare i rischi per i diritti delle persone interessate;
4. Fungere da punto di contatto per il Garante per la protezione dei dati personali e controllare che sia dato seguito alle richieste del Garante stesso.

Ancora, al secondo paragrafo l’art. 39 del GDPR con una formula prettamente di chiusura: “*Nell’eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell’ambito di applicazione, del contesto e delle finalità del medesimo*”, in sostanza con tale disposizione di portata generale si chiede al DPO di delineare un ordine di priorità nell’attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di

protezione dei dati.[20]

Il registro delle attività di trattamento

Rientrante a sua volta nel concetto di *accountability* risulta essere anche il cosiddetto Registro delle attività di trattamento, novità introdotta dall'art. 30 del GDPR.

Quest'ultimo altro non è che lo strumento attraverso il quale il titolare e il responsabile del trattamento documentano in forma scritta, anche elettronica, le principali informazioni relative alle attività di trattamento e alle misure di garanzia adottate, in base alle finalità perseguite ed ai profili di rischio rilevati, al fine di poter poi dimostrare all'Autorità di controllo (il Garante per la protezione dei dati) di aver adempiuto correttamente alla propria funzione di protezione dei dati personali.

Per quanto concerne propriamente l'ambito sanitario la regolare tenuta del Registro delle attività di trattamento risulta quale obbligo per tutti gli operatori sanitari (singoli professionisti sanitari, medici di medicina generale, ospedali privati, case di cura, farmacie, parafarmacie, Aziende Sanitarie appartenenti al S.S.N. *etc*.).

Per analizzarne nel dettaglio il contenuto minimo si guardi alla elencazione fornita all'art. 30 del Regolamento, in base al quale il Registro conterrà:

1. Il nome e i dati di contatto del titolare del trattamento;
2. Le finalità del trattamento (come "trattamento dei dati del paziente per l'erogazione della specifica prestazione sanitaria");
3. Una descrizione delle categorie di interessati (ad esempio "pazienti") e circa le categorie di dati

personali (quali dati anagrafici, dati biometrici *etc*.);
4. Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati (si pensi ad un laboratorio analisi);
5. Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
6. Ove possibile, una descrizione generale circa le misure di sicurezza tecniche ed organizzative adottate (quali *security policy*, sistemi di *intrusion detection etc*.).

Potrà ad ogni modo esser riportata nel registro qualsiasi informazione che il titolare od il responsabile ritengano utile dover indicare (come le valutazioni di impatto effettuate o le modalità di raccolta del consenso seguite).

Standard internazionali per la sicurezza dei dati: ISO 27001

Come si è potuto osservare poc'anzi la normativa europea pone in capo ai titolari e responsabili del trattamento dei dati numerosi adempimenti, fra i quali assume notevole rilievo l'adozione di "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*".

Così infatti dispone l'art. 32 del GDPR cercando di guidare la scelta di tale misure in base al principio di adeguatezza, nonché "*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 ed anche le libertà delle persone fisiche*".

Essendo tali ultime formule pressoché generali, l'esigenza attuale risulta quella di fornire ai titolari e ai responsabili del trattamento degli strumenti concreti per individuare e scegliere idonee misure di sicurezza ed essere in grado di dimostrane la pratica adozione.[21]

Nel classificare invero le misure di sicurezza adottabili il GDPR opera un riferimento a due categorie di misure: quelle tecniche e quelle organizzative, diversamente dalla letteratura del settore[22] che invece distingue in: misure volte a garantire la sicurezza organizzativa (quali procedure di gestione di *data breaches*), quelle relative alla sicurezza logica e tecnologica (quali sistemi di autenticazione, *antimalware*, *firewall*, monitoraggi, scansioni delle vulnerabilità), e quelle relative alla sicurezza fisica (si pensi alla sicurezza degli edifici e degli archivi, al controllo degli accessi ed alla sicurezza ambientale). L'obiettivo di tutte le anzidette misure sarà comunque quello di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi informativi.

Con l'obiettivo di agevolare la specifica scelta delle misure di sicurezza concretamente adottabili da parte del titolare e del responsabile del trattamento soccorrono sul piano internazionale le c.d. normative ISO, ossia norme tecniche sviluppate dalla *International Organization for Standardization* riportanti linee guida che un determinato soggetto dovrà andare a rispettare per l'ottenimento di una certificazione valida sul piano internazionale, attestante la conformità del soggetto stesso (persona fisica, ente pubblico o privato) a specifici parametri di valutazione.

Fra la molteplici norme ISO, si può qui porre in evidenza la ISO 27001 quale standard internazionale per la sicurezza delle informazioni, creata al fine di definire i requisiti atti a stabilire, implementare, mantenere e migliorare un sistema di gestione della sicurezza delle informazioni. [23]

Nei suoi contenuti presenta infatti un insieme di best practices, utili per sviluppare ed accrescere la capacità delle organizzazioni di gestire i rischi legati alla protezione dei dati, la ISO 27001 è invero molto specifica nel raccogliere, nel suo cosiddetto annex A, un vero e proprio catalogo di misure da adottare per contrastare nonché mitigare

i rischi di perdita, modifica, divulgazione non autorizzata od accesso ai dati personali trattati.

Non sarebbe del tutto errato pensare quindi alla normativa GDPR e alla ISO 27001 alla stregua di un sistema integrato in ambito di sicurezza dei dati, d'altronde è lo stesso *Considerando* 100 del GDPR ad incoraggiare "*l'istituzione di meccanismi di certificazione*" che possano consentire di valutare il livello di protezione dei dati prodotti e dei servizi.

Ed ancora, è l'art. 24, comma 3 del GDPR a specificare come l'adesione ai codici di condotta ed alle certificazioni approvate, proprio come la ISO 27001, possa essere considerata come un elemento dimostrativo circa la conformità ed il rispetto degli obblighi del titolare del trattamento, in ossequio allo stesso principio di *accountability*.

Purtuttavia pare ovvio sottolineare come la garanzia di una certificazione non reciderà mai del tutto il rischio di verificazione di eventi dannosi relativi alla sicurezza dei dati, come peraltro si constaterà a seguire in ambito sanitario, ma al massimo andrà ad attenuarne le possibilità ed eventualità di accadimento e, conseguentemente, le relative responsabilità per tutti coloro che trattano i dati e le informazioni.

Condizioni di liceità del trattamento in ambito sanitario

Rimane tuttora da chiarire cosa si debba intendere con la precisa locuzione "trattamento dei dati", di qui la definizione fornita dall'art. 4 del GDPR: "*Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la*

conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, ed altresì la cancellazione o la distruzione".

Si può evidenziare peraltro come una operazione di trattamento si articoli in differenti fasi: una preliminare (raccolta e registrazione), una di elaborazione (selezione, impiego), una di circolazione (o diffusione), ed infine una residuale (conservazione, cancellazione).

Si vuole sottolineare come l'art. 9 del GDPR ponga un divieto generale al trattamento di intere categorie particolari di dati, fra cui figurano proprio i dati relativi alla salute: "*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 ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*".

Tuttavia tale divieto non è certo assoluto, in quanto in presenza di tutta una serie di condizioni di liceità, espressamente elencate dallo stesso testo normativo, tale preclusione non opera.

Per ciò che ivi interessa, il trattamento dei dati sanitari sarà considerato lecito laddove avvenga: per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale (cosiddetta "finalità di cura"); per motivi di interesse pubblico nel settore della sanità pubblica (si pensi alla gestione di emergenze sanitarie nazionali, od alla protezione da gravi minacce per la salute a carattere transfrontaliero); ed ancora a fini di archiviazione nel pubblico interesse, di ricerca scientifica, storica o a fini statistici.

Vale la pena soffermarsi su come di fatto il GDPR superi così la precedente cornice normativa "consensocentrica" (propria del d.lgs. 196/2003, Codice privacy): diversamente dal passato infatti, non dovrà più esser richiesto il consenso del paziente per il trattamento di dati in ambito sanitario, purché si tratti di dati specificatamente necessari alle "finalità di cura" previste dal Regolamento Ue (prevenzione, diagnosi *etc*.) e che le relative attività siano effettuate da un professionista sanitario soggetto al segreto professionale.

Così, per esemplificare, persegue una finalità di cura l'infermiere che effettua una valutazione dei parametri vitali di un paziente al momento dell'accesso in pronto soccorso, come anche il cardiologo che raccoglie l'anamnesi necessaria alla corretta refertazione di un elettrocardiogramma; lo specialista che annota i dati biometrici del paziente in vista di un intervento chirurgico, come pure, in senso ampio, un direttore sanitario di una struttura pubblica che procede alla archiviazione di dati per studi statistici finalizzati tutela della salute collettiva.[24]

Ovvio è, ma vale la pena specificarlo, che non si deve qui confondere il consenso prestato al trattamento dei dati sanitari, col consenso ai trattamenti sanitari stessi: è quest'ultimo infatti a costituire il presupposto di legittimità dell'operato medico, andando ad "assorbire" il primo consenso, che non risulta più pertanto necessario.

D'altronde un professionista sanitario dovrà necessariamente venire a conoscenza di tutta una serie di dati identificativi e clinici (anamnesi, farmaci assunti *etc*.) per l'esecuzione di un trattamento sanitario, ed egli stesso, d'altra parte, nel trattare il paziente andrà a generare tutta un'altra serie di dati (referti, lastre *etc*.), dal momento poi che la semplice raccolta e consultazione di dati ne costituisce per definizione un trattamento, per un medico risulterà inevitabile, nello svolgimento delle sue funzioni, trattare costantemente i dati personali dei pazienti.

Si segnali ancora come ai trattamenti “per finalità di cura” siano comunque equiparati anche i trattamenti operati tramite applicazioni mediche, quando la finalità perseguita è quella di fornire cura al paziente, tramite un servizio di telemedicina, telesorveglianza o telemonitoraggio.

È evidente inoltre come tale dispensa dall’ottenimento del consenso non opererà laddove i trattamenti dei dati dei pazienti avvengano per finalità diverse da quelle strettamente di cura (si pensi a fini promozionali, commerciali o di fidelizzazione della clientela).

Residuano ad ogni modo alcuni casi in cui i dati sanitari possono essere trattati esclusivamente con il consenso della persona interessata quali: come si diceva nel primo capitolo, la possibilità di accesso al FSE (fascicolo sanitario elettronico), l’adesione a servizi di refertazione online, oppure l’utilizzo di *apps* mediche, quando il trattare i dati del paziente afferisce, solo in senso lato, alla cura di quest’ultimo, ma non è ad essa strettamente necessario (si pensi ad una applicazione che fornisce indicazioni su come migliorare la qualità del sonno), in tal caso il titolare del trattamento dovrà trattare i dati previa acquisizione del consenso dell’utente interessato.

Si può concludere evidenziando come l’approvazione del GDPR abbia indubbiamente contribuito a richiamare l’attenzione degli operatori sanitari sui temi della privacy e della protezione dei dati, in quanto strettamente connessi ai profili della sicurezza delle cure e di dignità del paziente. Come evidenziato infatti dal Garante, nella sua relazione annuale al Parlamento dell’anno 2018,[25] eventuali carenze in ambito di sicurezza dei dati personali possono avere effetti oltremodo deleteri negli stessi processi di erogazione dei trattamenti medici, rappresentando causa di disfunzioni, rallentamenti ed errori sanitari, fonti di potenziale responsabilità della struttura sanitaria, obbligata così a risarcirne i danni conseguenti.

L’obbiettivo di questi due preliminari capitoli voleva essere il presentare la digitalizzazione della sanità quale occasione senza precedenti di sviluppo ed innovazione, da dover senza dubbio promuovere per una sempre maggiore efficienza ed universalità delle cure, e per una migliore programmazione della spesa sanitaria. Tuttavia suddetta *digital health* dovrà realizzarsi all’interno di un progetto di politiche pubbliche organico e lungimirante di governance sanitaria, che promuova una condivisione selettiva dei dati sanitari, con le dovute cautele, al fine di minimizzarne i rischi cibernetici e le conseguenti possibili lesioni alla sfera personale della riservatezza e della dignità dei pazienti.[26]

La sanità digitale, pur rappresentando un’occasione di sviluppo e innovazione, espone inevitabilmente a rischi di compromissione dei sistemi informativi e alla minaccia crescente della cybercriminalità. Proprio a questo tema sarà dedicato il prossimo articolo della serie, che introdurrà la rivoluzione digitale e l’innovazione criminale, approfondendo le nuove forme di criminalità tecnologica.

Per approfondire, invitiamo a leggere il white paper gratuito di **Maria Vittoria Zucca** dal titolo “**La cybercriminalità nel settore sanitario: anamnesi, diagnosi e prognosi di una ‘patologia’ informatica”.**

Fonti:

[1] A. Salvadori, “Deontologia e tutela dei dati sanitari”, in Torino Medica. La rivista dell’ordine dei medici chirurghi e odontoiatri della provincia di Torino, anno XXXIII, numero 3-4, 2021, pp. 9-10.

[2] ANITEC-ASSINFORM (Associazione italiana per l’Information and Communication Technology), Una data strategy per la Sanità italiana, a cura del gruppo di lavoro Digital Transformation in Sanità di Anitec-Assinform, Maggio 2022, p. 20.

[3] Intervento di A. Soro, ex-presidente dell’Autorità Garante

per la protezione dei dati personali, “Tracciamento contagi coronavirus, ecco i criteri da seguire”, in Agenda Digitale, 29 Marzo 2020.

[4] L’immagine della scala delle durezze, diffusamente ripresa nella dottrina che si è occupata di privacy, si deve a Stefano Rodotà. Cfr. S. Rodotà, “Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali”, in Rivista critica del diritto privato, anno XV, 1997, pp. 583-609.

[5] F. Di Ciommo, “Il trattamento dei dati sanitari tra interessi individuali e collettivi”, in R. Pardolesi (a cura di), La privacy sanitaria, vol. II, Giuffrè editore, Milano, 2003, vol. II, p. 239.

[6] Regolamento (Ue) 2016/679 del Parlamento e del Consiglio, relativo alla “protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”, del 27 Aprile 2016, che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), per il testo normativo nella sua completezza si rimanda al sito internet: eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679.

[7] Decreto legislativo 30 Giugno 2003, n. 196, recante il “Codice in materia di protezione dei dati personali”, integrato con le modifiche introdotte dal decreto legislativo 10 Agosto 2018, n. 101, recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (Ue) 2017/679 del Parlamento e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

[8] Intervento di P. Stanzione, Presidente dell’Autorità garante per la protezione dei dati personali, “Sicurezza del dato sanitario e condivisione”, in Panorama, 18 Febbraio 2022.

[9] Il documento Indicazioni nazionali per l’erogazione di

prestazioni di telemedicina è stato approvato dalla Cabina di regia del NSIS nella seduta del 28 ottobre 2020 ed è stato adottato con Accordo in Conferenza Stato Regioni del 17 dicembre 2020 (Repertorio atti n.215/CSR).

[10] NETPATROL, op. cit. supra a nota 17, p. 8.

[11] G. D'Acquisto, M. Naldi, Big Data e Privacy by Design. Anonimizzazione, Pseudonimizzazione e Sicurezza, Giappichelli Editore, Torino, 2017.

[12] A. Antonilli, op. cit. supra a nota 3, p. 92.

[13] Per "titolare del trattamento" si rimandi all'art 4 del GDPR: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali […]".

[14] P. Perri (intervento), durante il Webinar "Conoscere e prevenire gli attacchi cyber in sanità", tenutosi in data 30 giugno 2021.

[15] Per "interessato" si intenda la persona fisica alla quale si riferisce il dato personale.

[16] D. Poletti, "Comprendere il Reg. UE 2016/679: Un'introduzione", in A. Mantelero, D. Poletti (a cura di), Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna, Pisa University Press, 2018, pp. 9-19.

[17] A. Cortesi, "L'art. 25 del GDPR: dalla privacy by default al principio di minimizzazione o necessità nel trattamento dei dati personali", in Interlex: rivista di diritto, tecnologia, informazione, 2017.

[18] NETPATROL, op. cit. supra a nota 17, p. 9.

[19] Per "responsabile del trattamento" si rimanda all'art. 4

del GDPR: “la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.”

[20] “Linee guida sui responsabili della protezione dei dati”, WP243 rev. 01, adottate dal Gruppo di lavoro articolo 29 in materia di protezione dei dati personali, versione emendata ed adottata il 5 aprile 2017.

[21] R. Riccio, “Le misure di sicurezza tra GDPR e ISO 27001: due normative a confronto e i possibili scenari prospettabili”, in Cyberlaws: free legal database and blog, 9 Gennaio 2019.

[22] G. Butti, A. Piamonte, GDPR: nuova privacy. La conformità su misura, Iter editore, Milano, 2017.

[23] ISO/IESC 27001: 2013, “Information technology – Security techniques – Information Security – Managements systems – Requirements”.

[24] G. Chiarini, “Privacy: come cambia il dato normativo”, in E-Health: innovazione e tecnologia in ospedale, vol. 72, 2019, pp. 66-69.

[25] La Relazione del Garante per la protezione dei dati sanitari al Parlamento del 2018 è reperibile qui.

[26] P. Stanzione, intervento cit. supra, a nota 32.

Profilo Autore

Maria Vittoria Zucca, laureata con lode in Giurisprudenza presso l’università degli Studi di Trento, è attualmente dottoranda nel Programma di Dottorato di Interesse Nazionale in Cybersecurity, con istituzione capofila la Scuola IMT Alti Studi di Lucca, ed è affiliata alla Scuola Superiore Sant’Anna, presso l’Istituto Dirpolis (Diritto, Politica e Sviluppo).

La sua attività di ricerca si concentra sulla prevenzione, l’indagine ed il contrasto della criminalità informatica, includendo le discipline del diritto penale dell’informatica e della criminologia digitale. Su questi temi è autrice di diverse pubblicazioni scientifiche e partecipa regolarmente a conferenze nazionali e internazionali.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/dati-sanitari/