Intervista al dott. Simone Paolucci, DPO Officer Humanitas

Andrea d'Agostino
LL.M., Avvocato Senior Legal Counsel e Responsabile Privacy del Gruppo Mondadori. Vice Presidente dell'Unione Giuristi per l'Impresa

Privacy& ha incontrato il dott. Simone Paolucci, Data Protection Officer Humanitas, con l'intento di approfondire le peculiarità e le complessità del sistema di gestione delle attività di trattamento di dati personali all'interno di uno dei principali gruppi ospedalieri del paese.

Humanitas è un gruppo di ospedali ad alta specializzazione, un Centro di Ricerca punto di riferimento mondiale per la ricerca sulle malattie legate al sistema immunitario, e Humanitas University, Ateneo internazionale dedicato alle Life Sciences.

Circa 1 milione di pazienti ogni anno scelgono di affidarsi agli specialisti degli ospedali Humanitas, presenti a Rozzano, Milano, Castellanza, Bergamo, Torino e Catania.

Humanitas è sul territorio anche con numerosi centri medico-diagnostici e punti prelievi, Humanitas Medical Care.

Il dott. Simone Paolucci, specializzato in *Privacy Law, Health Law, Legal Informatics, New Technologies Law, HealthCare Information Technology*, è esperto conoscitore da più di 15 anni degli aspetti di protezione dei dati personali e sicurezza delle informazioni nell'ambito sanitario sia privato che pubblico, riveste il ruolo di Data Protection Officer di Humanitas e di Humanitas University dall'inizio del 2018.

È docente in materia di protezione dei dati personali in Corsi di Specializzazione e Master.
Per la prima volta Privacy& è lieta di intervistare il Data Protection Officer di un gruppo ospedaliero approfondendo le complessità sottese alla gestione di dati personali, soprattutto afferenti a categorie particolari di dati personali ex articolo 9 del Regolamento UE 2016/679, in ambito sanitario nonché all'utilizzo di strumenti tecnologi avanzati, ivi inclusa l'intelligenza artificiale, per effettuare attività di trattamento particolarmente complesse e delicate vista la natura dei dati trattati.

Q: Benvenuto e grazie per aver accettato l'invito della nostra redazione a prendere parte a questo stimolante confronto. Inizierei subito con una domanda apparentemente banale ma in realtà estremamente interessante: come si svolge la sua giornata tipo all'interno di Humanitas e quali sono le tematiche più ricorrenti per le quali è richiesto l'intervento del Data Protection Officer?
Dott. S. Paolucci: Grazie a voi per l'opportunità concessami di far conoscere tematiche così importanti e complesse legate all'utilizzo dei dati nel mondo sanitario.
Difficile poter descrivere una giornata tipo in quanto le attività quotidiane sono spesso diverse e le richieste da parte dei colleghi degli Ospedali Humanitas arrivano all'improvviso e richiedono analisi e risposte ragionate e tempestive. Chiaramente, essendo il mio un ruolo di indirizzo e di "consulenza" interna, sono chiamato a valutare dal punto di vista della protezione dei dati personali le nuove iniziative e i nuovi progetti che si intendono realizzare e ad esprimere pareri. Pertanto la raccolta e valutazione delle informazioni, insieme all'analisi e interpretazione della normativa di riferimento per una sua corretta applicazione, sono le attività più ricorrenti in una giornata tipo. In questo momento le tematiche più ricorrenti sono sicuramente quelle legate all'allenamento e utilizzo di algoritmi di Intelligenza Artificiale nel mondo della ricerca clinica e scientifica, con particolare riferimento alle patologie relative al Covid-19. Altro argomento sul quale si sta concentrando l'attenzione è la valutazione dei servizi di telemedicina, con particolare riferimento alle televisite e ai teleconsulti clinici in modo da facilitare i pazienti evitando loro, se non strettamente necessario, di raggiungere fisicamente le strutture ospedaliere, in un periodo particolarmente delicato come quello attuale.
Per tutte queste attività l'attuazione dei principi e delle regole di data protection by design e by default e le correlate analisi dei rischi privacy sono elementi di fondamentale importanza per la realizzazione di servizi conformi alle normative di settore.

L'altra attività specifica del DPO, direi la principale che svolgo regolarmente, è il monitoraggio e la verifica costante dell'osservanza della normativa in materia di protezione dei dati personali, nonché delle politiche definite dal Titolare del trattamento, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.
Questa attività si sostanzia anche nella definizione e svolgimento di audit interni alle singole Strutture del Gruppo e nella messa in atto di simulazioni di data breach.

Q: Considerata la vastità e complessità delle attività di trattamento condotte dal Gruppo Humanitas, quale sistema di gestione della privacy avete adottato per dar corso ad una concreta attuazione del principio di accountability?
Dott. S. Paolucci: Il sistema di gestione della protezione dei dati personali di Humanitas è caratterizzato da una Data Protection Policy sintetica che riassume ruoli, responsabilità, processi organizzativi e gestionali, rimandando a singole procedure o linee guida di dettaglio relative alla data protection by design e by default, all'analisi dei rischi, alla gestione dei data breach, all'aggiornamento del registro delle attività di trattamento, alla gestione dei diritti degli interessati.
Le singole procedure sono corredate da infografiche sintetiche che vengono distribuite a tutto il personale perché possa essere informato, formato e sensibilizzato a riguardo.
Inoltre, per alcuni servizi o attività specifiche ritenute importanti dal punto di vista della protezione dei dati personali, vengono redatte apposite schede di accountability in merito alle valutazioni condotte e alle indicazioni suggerite.
Nel pieno rispetto del principio di accountability e delle indicazioni di carattere generale che l'Autorità Garante per la Protezione dei Dati Personali ha dispensato nelle more del passaggio dalla precedente alla nuova normativa, Humanitas ha adottato un sistema "binario" per la gestione dei dati personali, distinguendo nettamente la figura del DPO da quella del responsabile privacy (intesa come figura operativa che caratterizza le scelte del titolare del trattamento). Pertanto la mia figura (DPO) gode di una piena e totale indipendenza rispetto alla struttura del titolare del trattamento: in questo modo l'attività di controllo propria di questo ruolo viene svolta scrupolosamente e senza influenze. Ad una collega è invece stato affidato l'altrettanto stimolante ruolo di affiancare ogni singolo titolare del trattamento del Gruppo Humanitas nell'attuazione delle scelte che contemplano attività di trattamento di dati personali e che sono riportate all'interno degli appositi Registri.

Q: Con l'avvento del GDPR uno dei temi che ha acquisito sempre più rilevanza all'interno delle aziende è stata la gestione dei diritti degli interessati. Sul punto come si è organizzato il Gruppo Humanitas?
Dott. S. Paolucci: Il rapporto con gli interessati e la corretta gestione dei loro diritti è un punto fondamentale per Humanitas, da sempre attenta alla sicurezza e alla qualità di ogni particolare del percorso di cura che offre ai propri pazienti.
A tale proposito presso le aree di attesa sono presenti cartelli con l'informativa sul trattamento dati contenente i diritti degli interessati e le modalità di esercizio; è stata inoltre predisposta un'apposita pagina web sui vari siti internet dei singoli ospedali all'interno della quale sono pubblicate tutte le informazioni relative alla protezione dei dati e dove è presente un apposito form per l'esercizio dei diritti da parte degli interessati.
Per la gestione dei diritti degli interessati è stata redatta un'apposita procedura che definisce il corretto flusso delle richieste dalla ricezione, alla presa in carico, all'evasione, assegnando ad ogni professionista che partecipa al percorso di cura ruoli, responsabilità e tempistiche.
Le richieste vengono gestite dal Referente Privacy che lavora a stretto contatto con il DPO e raccoglie tutte le informazioni necessarie per rispondere all'interessato, con la collaborazione delle varie Funzioni coinvolte.
È stato inoltre definito un apposito Registro delle richieste che consente di tenere traccia delle istanze, delle varie Funzioni coinvolte e delle risposte fornite.
Questo assetto ci ha permesso di gestire in maniera puntuale le richieste di esercizio dei diritti degli interessati che, per la natura delle attività svolte dal nostro Gruppo, sono sempre state poco ricorrenti ma estremamente puntuali. A favorire una tale situazione vi è stata anche l'impostazione che abbiamo deciso di dare alle informative ex articolo 13 del GDPR rese a tutti i nostri interessati. Sposando appieno lo spirito del legislatore europeo e di tutte le autorità di controllo, abbiamo prestato particolare attenzione al linguaggio di tali documenti e, ove possibile, abbiamo introdotto elementi iconografici che rendono i contenuti semplici e intuitivi. La trasparenza nei confronti degli interessati ed il rapporto di fiducia instaurato negli anni tra questi e Humanitas ha contribuito a rendere i meccanismi di gestione della privacy in azienda sempre più fluidi ed efficaci.

Q: Tra tutti i settori, quello sanitario è sempre stato quello forse più esposto al fenomeno del data breach in considerazione anche alla natura dei dati trattati. In un tale contesto, il data protection officer ricopre un ruolo determinate nel supportare il titolare del trattamento sia nella

fase organizzativa/procedurale sia nella fase patologica a data breach avvenuto. Con quale spirito e con quali azioni è riuscito in questi anni a supportare il Gruppo Humanitas nella gestione dei data breach?
Dott. S. Paolucci: L'argomento è molto delicato e necessita sempre la massima attenzione. Quando si riscontra un incidente che può qualificarsi come violazione di dati, le attività in corso del DPO si fermano e la concentrazione è tutta rivolta all'analisi di quanto accaduto.
Prima di gestire un data breach occorre che questo venga innanzitutto correttamente rilevato e comunicato al DPO. Pertanto, a seguito della definizione della procedura di gestione dei data breach è stata lanciata una campagna di sensibilizzazione tra tutti i professionisti attraverso videoclip sul tema e infografiche dedicate, mostrando esempi concreti di data breach e le prassi operative da seguire nel caso si riscontrassero tali situazioni.
In aggiunta, ad ogni evento di formazione, viene sempre trattato l'argomento specifico del data breach, sensibilizzando ulteriormente gli operatori, mostrando anche le conseguenze di eventuali comportamenti scorretti da parte loro e richiamandoli alla massima attenzione nello svolgimento delle proprie mansioni.
Sul piano concreto Humanitas ha adottato una struttura organizzativa privacy piuttosto ramificata tramite specifiche attività di formazione e responsabilizzazione di diverse persone chiave all'interno del Gruppo. Queste hanno anche il compito di allertare il DPO ogni qual volta venga riscontrata un'anomalia che impatti sulla protezione dei dati personali e possa essere identificata come data incident o data breach.

Q: Anche se piuttosto scontata non posso astenermi dal farle una domanda in merito all'emergenza pandemica che purtroppo stiamo ancora vivendo. Riuscirebbe a raccontarci in che modo e con quali attività il Gruppo Humanitas ha affrontato l'emergenza sanitaria da Covid-19 nella gestione dei dati personali?
Dott. S. Paolucci: Come il mondo sanitario di fronte all'emergenza Covid-19 ha dovuto fare i conti con i propri limiti e le proprie carenze, anche gli "addetti" alla protezione dei dati personali hanno dovuto misurarsi con i limiti e le imperfezioni della normativa di settore, inizialmente non in grado di fronteggiare la situazione.
Questo ha condotto a una forte interpretazione delle vigenti normative per poter venire incontro alle esigenze emergenziali degli ospedali, fino a quando l'Autorità Garante per la Protezione dei dati personali non ha fornito indicazioni specifiche a riguardo.
Gli ospedali hanno dovuto cambiare "forma" e organizzazione molto rapi-

damente durante le varie ondate pandemiche e di conseguenza anche molti aspetti sul trattamento dei dati sono stati rivisti rispetto ai percorsi tradizionali. L'accesso alle strutture è stato contingentato e i pazienti e i dipendenti sono stati sottoposti a rilevazione della temperatura corporea con termoscanner e di conseguenza ci si è trovati ad analizzare e affrontare aspetti di protezione dei dati nuovi. Per tutti questi nuovi trattamenti sono stati applicati i principi di privacy by design e privacy by default e sono state seguite tutte le procedure interne per la gestione di nuove attività di trattamento. Ciò ci ha permesso di testare e migliorare ulteriormente gli ingranaggi del nostro sistema privacy e l'applicazione del principio di accountability.
Molti servizi sanitari ordinari sono state sospesi e si è dovuto affrontare il passaggio alle televisite laddove possibile con notevoli implicazioni di sicurezza e privacy da indirizzare e gestire.
I nostri ospedali hanno vaccinato i propri professionisti e hanno aperto centri vaccinali per i cittadini del territorio ed i pazienti fragili e pertanto ci si è dovuti misurare con nuovi servizi mai offerti prima, valutando nuovi aspetti di protezione dei dati bilanciandoli con le esigenze di prevenzione.

Q: In conclusione le chiederei qualche spunto in tema di sicurezza e protezione dei dati personali. In particolare, con riferimento allo smart-working incentivato, nel bene o nel male, dall'emergenza pandemica, in che modo siete riusciti ad organizzarvi nel consentire il trattamento di dati sanitari a distanza in totale sicurezza?
Dott. S. Paolucci: L'emergenza pandemica ha sicuramente favorito e accelerato alcuni processi già in fase di attuazione, come ad esempio la connessione da remoto ad applicazioni e servizi degli ospedali in totale sicurezza. Sono state definite regole di comportamento con precise indicazioni e istruzioni per lo smart-working, in modo da garantire riservatezza e sicurezza nello svolgimento delle attività lavorative fuori sede, anche attraverso una serie di moduli di formazione a distanza.
Si è assistito quindi ad un rapido rafforzamento delle misure di sicurezza tecniche ed operative, anche attraverso sistemi di VPN a due fattori di autenticazione e l'utilizzo di dispositivi mobili sicuri. Nell'ottica del principio di accountability possiamo sostenere che l'emergenza pandemica ha contribuito, quindi, a migliorare ulteriormente il sistema organizzativo di Humanitas nonché, come dicevo, a rafforzare le misure di sicurezza sia tecnologiche sia organizzative, proprio al fine di prevenire eventi che possano avere impatto sulla sicurezza e protezione dei dati personali trattati.