TAKE HOME MESSAGE

L'ALCHIMIA DEI DATI: trasparenza e responsabilità nella cura e nella ricerca clinica.

Sala Conferenze Ordine Medici Chirurghi e Odontoiatri di Brescia – Mercoledì 3 giugno 2026.

DESCRIZIONE DELL'INIZIATIVA

Il convegno ha affrontato il delicato equilibrio tra l'evoluzione tecnologica e la tutela del dato sanitario alla luce del GDPR e delle recenti direttive del Garante della Privacy. L'avvento della sanità digitale — dal consolidamento del Fascicolo Sanitario Elettronico (FSE) all'istituzione dell'Ecosistema dei Dati Sanitari (EDS) — offre straordinarie opportunità di cura e ricerca, ma impone il passaggio da un mero "adempimento formale" a una vera e propria "responsabilità attiva" (accountability) del professionista.

In parallelo, i relatori hanno analizzato l'impatto della digitalizzazione sulla percezione della salute pubblica: l'attuale panorama informativo, caratterizzato da fenomeni di infodemia, proliferazione di fake news veicolate da social network e algoritmi di intelligenza artificiale, rischia di generare "epistemia" (una pericolosa illusione di conoscenza) ed effetti di disaffezione medica, come la cybercondria. I medici e gli operatori sanitari sono dunque chiamati non solo a proteggere rigorosamente il "corpo elettronico" dei pazienti attraverso un'ineccepibile gestione del dato, ma anche a farsi promotori attivi di una comunicazione scientifica trasparente, rigorosa e metodologicamente fondata, per contrastare la deriva della disinformazione globale.

PUNTI CHIAVE

- **Dati "Particolari" e Basi Giuridiche:** Il GDPR (Art. 9) vieta la gestione dei dati sulla salute, salvo specifiche deroghe. Per le **finalità di cura,** svolte da professionisti sanitari sotto segreto professionale, **non serve il consenso** per le prestazioni ordinarie. Il consenso esplicito e una tantum resta invece indispensabile per la consultazione del FSE, referti online o uso di app mediche. Per l'interesse pubblico rilevante (certificazioni, medicina legale, obblighi di denuncia), la base giuridica è la legge, non il consenso.

- **La Deroga per la Ricerca Scientifica** (Art. 110): Negli studi clinici o epidemiologici la regola d'oro è la raccolta del consenso specifico. Negli studi retrospettivi, qualora informare l'interessato risulti impossibile (es. pazienti deceduti) o comporti uno sforzo sproporzionato/grave pregiudizio alla ricerca, si può derogare solo attivando precisi pilastri: stesura di un protocollo motivato, parere favorevole del Comitato Etico, esecuzione e pubblicazione di una Valutazione d'Impatto sulla protezione dati (Data Protection Impact Assessment: DPIA) e notifica al Garante. Per i pazienti non contattabili, il medico deve comprovare e registrare i "ragionevoli sforzi" di tracciamento effettuati.

- **Prevenzione del Data Breach:** La violazione della sicurezza dei dati (distruzione, perdita, modifica o divulgazione illecita) espone la struttura a pesanti sanzioni del Garante. Gli errori più frequenti includono lo scambio o la consegna di referti a omonimi, lo smarrimento di diarie cliniche o cartacee e l'invio di messaggi elettorali a liste di pazienti visibili. Il Titolare deve notificare l'evento al

Garante entro 72 ore dalla scoperta, a meno che sia improbabile un rischio per i diritti degli interessati. Se il rischio è elevato, la violazione va comunicata tempestivamente anche al paziente. Ogni incidente va obbligatoriamente mappato nel Registro dei Data Breach.

- **L'Infodemia e la Sfida della Verità:** I social media e la GenAI amplificano la diffusione di spiegazioni ingannevoli che risultano spesso più persuasive dei dati scientifici ufficiali. Il 35% delle persone (con picchi tra i giovani) ritiene che un cittadino comune, compiendo ricerche autonome online, possa acquisire competenze pari a quelle di un medico. I palinsesti informativi personali e le *echo chambers* digitali polarizzano le opinioni e acuiscono la sfiducia nella medicina.

CONCLUSIONI

La conformità alle normative sulla privacy non rappresenta un mero ostacolo burocratico, bensì una componente intrinseca dell'etica medica contemporanea. Come ricordato nella metafora del passaggio dall'habeas corpus all'habeas data, proteggere le informazioni sanitarie di un paziente significa oggi proteggere la sua stessa identità e dignità individuale.

L'attivazione di studi clinici o l'ordinaria operatività di cura richiedono una costante collegialità decisionale con il DPO, gli Uffici Privacy e i Comitati Etici, supportata da pratiche rigorose di minimizzazione, pseudonimizzazione e tracciamento sicuro dei dati. Al contempo, di fronte all'avanzata della disinformazione digitale e della spettacolarizzazione della scienza, la comunità medica ha il dovere di occupare l'arena comunicativa investendo risorse per tradurre i dati scientifici in messaggi fruibili, limpidi e autorevoli, capaci di ripristinare la necessaria alleanza di fiducia con la cittadinanza.

INFORMAZIONI UTILI

- **Sicurezza nei canali di messaggistica:** L'uso di chat generiche per scambiare foto, referti o diagnosi identificabili è illecito, anche in presenza di consenso del paziente, per assenza di log e controllo accessi. Consentito unicamente il consulto anonimo tra colleghi o comunicazioni logistiche.
- **Adempimento cardine studio retrospettivo**: È vietato avviare l'estrazione o l'analisi dei data-base clinici senza aver prima ottenuto il parere favorevole del Comitato Etico Territoriale (CET) e aver approvato/pubblicato la DPIA.

Per approfondimenti consulta il materiale del convegno sul sito dell'Ordine dei Medici
www.ordinemedici.brescia.it