LEGAL HEALTH

Regolamenti Ue sui dispositivi medici e GDPR: i nodi che l'Italia dovrà affrontare

Il nostro Paese si appresta ad adeguare il quadro normativo nazionale ai Regolamenti Ue in materia di dispositivi medici. Cruciale è il coordinamento con il Gdpr per quanto attiene al trattamento dei dati personali. Vediamo gli snodi più critici, anche in ambito cybersecurity

Pubblicato il 04 Giu 2021

Laura Liguori
Partner di Portolano Cavallo

Elisa Stefanini
Partner di Portolano Cavallo

Condividi

Articoli correlati

Prossimo
GPT-4, per alleggerire il lavoro dei medici: r

A valle dell'applicazione del regolamento europeo sui dispositivi medici (regolamento UE n. 745 del 2017), avvenuta il 26 maggio, l'Italia muove i primi passi per l'adeguamento del quadro normativo nazionale in materia. Così, la legge di delegazione europea 2021, pubblicata in Gazzetta Ufficiale lo scorso 23 aprile, ha dedicato un intero articolo (l'art. 15) proprio alla futura **disciplina dei dispositivi medici**, fornendo al Governo **principi e criteri** direttivi per l'adeguamento delle norme interne ai regolamenti europei.

Tra questi principi, tutti di notevole interesse nell'ottica di una ridefinizione della **governance dei dispositivi medici** in Italia, ci concentriamo oggi su quello che riguarda il coordinamento tra i regolamenti sui dispositivi medici e il regolamento (UE) n. 2016/679 sulla protezione dei dati personali ("**GDPR**").

Infatti, secondo i principi direttivi stabiliti dalla **legge di delegazione**, il Governo dovrà adeguare i trattamenti di dati personali effettuati in applicazione del regolamento sui dispositivi medici (e di quello sui dispositivi medico diagnostici in vitro n. 746/2017) alle disposizioni del GDPR e alla normativa vigente in materia di tutela dei dati personali.

Tale riferimento è estremamente importante in quanto pone l'attenzione su uno dei nodi cruciali circa la raccolta, la sicurezza e il trattamento dei dati sanitari effettuata da dispositivi medici.

Indice degli argomenti

La cybersecurity requisito essenziale di un dispositivo medico

Con il costante aumento di dispositivi medici che trattano grandi quantità di **dati personali** relativi alla salute, nella maggior parte dei casi connessi alla rete, inclusi i casi sempre più frequenti di dispositivi medici che sono costituiti unicamente da software o app (i cosiddetti "Software as Medical Devices" – SaMD), è evidente come la corretta gestione di questi dati diventi un fondamentale requisito di sicurezza del dispositivo medico, che non può non essere oggetto di una specifica valutazione.

A tale riguardo, l'allegato I del regolamento sui DM riporta tra i requisiti generali di sicurezza e progettazione che devono essere soddisfatti dai dispositivi contenenti un software o dai software che costituiscono dispositivi a sé stanti, le seguenti disposizioni:

1. il software deve essere **sviluppato e fabbricato** conformemente allo stato dell'arte, tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione del rischio, compresa la sicurezza delle informazioni, della verifica e della convalida (par. 17.2);
2. i fabbricanti indicano i **requisiti minimi** in materia di *hardware*, caratteristiche delle reti informatiche e misure di sicurezza informatica, compresa la protezione contro l'accesso non autorizzato, necessari per far funzionare il *software* come previsto (par. 17.4);
3. i dispositivi devono essere progettati e fabbricati in modo tale da proteggerli, per quanto possibile, da **accessi non autorizzati** che potrebbero impedire loro di funzionare come previsto (par. 18.8).

Ciò significa che tutti i dispositivi medici immessi sul mercato devono assicurare il rispetto (tra gli altri) dei punti che precedono come requisiti essenziali di sicurezza e prestazione che saranno oggetto di valutazione ai fini della marcatura CE del dispositivo.

A riprova della delicatezza e dell'importanza del tema, il **Medical Device Coordination Group** ("MDCG") della Commissione europea ha pubblicato, nel gennaio 2020, una "Guidance on Cybersecurity for medical devices", ossia linee guida che mirano a fornire ai fabbricanti di dispositivi indicazioni su come soddisfare tutti i **requisiti essenziali di cybersecurity** previsti dall'allegato I dei regolamenti. Inoltre, tali linee guida tengono conto del fatto che i nuovi regolamenti estendono certi obblighi anche a importatori e distributori, ampliando il novero dei soggetti che sono chiamati, attraverso una reciproca collaborazione, a realizzare gli obiettivi qualitativi imposti dai regolamenti stessi. Al riguardo, si sottolinea come la cybersecurity deve essere parte del sistema di **sorveglianza post-market** dei dispositivi medici, che il fabbricante deve realizzare con il coinvolgimento di tutti i soggetti della filiera al fine di poter porre in essere, in modo tempestivo, tutte le opportune azioni correttive.

Peraltro, l'importanza della cybersecurity in ambito sanitario è stata recentemente ribadita anche dall'Agenzia dell'Unione europea per la sicurezza informatica ("ENISA") che, il 18 gennaio 2021, ha pubblicato un documento volto a incentivare le organizzazioni sanitarie ad adottare servizi *cloud* seguendo tutte le misure di sicurezza necessarie. Nel documento si evidenzia infatti come rischi di intrusioni esterne e di minacce alla sicurezza informatica sono ancora più probabili laddove le strutture sanitarie si appoggino a fornitori di *cloud* esterni per raccogliere i dati provenienti dai dispositivi medici utilizzati ai fini del monitoraggio da remoto dei pazienti.

Il rapporto con il GDPR

Pur sottolineando l'importanza della cybersecurity come requisito di sicurezza dei dispositivi, i regolamenti non entrano nel dettaglio del **rapporto con la normativa sulla protezione dei dati personali** e su come si debbano coordinare le rispettive previsioni normative.

Se i regolamenti non menzionano neppure il GDPR, le **linee guida sulla cybersecurity** includono nella lista di requisiti di sicurezza informatica che devono essere soddisfatti dagli operatori del settore anche il rispetto delle norme nazionali ed europee, incluso il GDPR (oltre che l'EU Cybersecurity Act n. 881/2019).

della certificazione di un dispositivo medico.

La necessità di un coordinamento anche a livello europeo

In quest'ottica, è evidente come la disposizione di cui all'art.15 della legge di delegazione europea menzionata in precedenza appaia di estrema attualità. Sarà, infatti, importante vedere quali saranno, in concreto, le **norme adottate dal Governo** per assicurare il rispetto della normativa sulla protezione dei dati sanitari nel contesto dei trattamenti effettuati con l'impiego di dispositivi medici. Ciò dovrà avvenire mediante l'adozione di uno o più decreti legislativi entro i prossimi 12 mesi.

Trattandosi peraltro di un tema che coinvolge l'attuazione di regolamenti europei, si auspica che in futuro vengano forniti ulteriori chiarimenti anche a livello europeo, in modo da evitare, in una materia così sensibile, che si possano creare disparità tra Stati membri nell'attuazione dei regolamenti tali da generare incertezze e ulteriori complessità per gli operatori del settore.

* *Si ringrazia Giulia Conforto per aver contribuito alla realizzazione di questo articolo*

Valuta la qualità di questo articolo