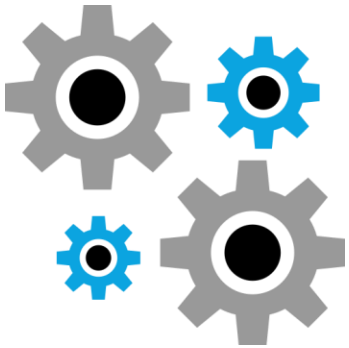
AIIC 2024 AWARDS

ARES Sardegna

«Contratti di fornitura di dispositivi medici connessi a piattaforme telematiche: focus sulle responsabilità nel trattamento dei dati personali e particolari»

AIIC associazione italiana ingegneri clinici

Il gruppo di lavoro



Dott. Giovanni Scarteddu
ARES Sardegna – S.S. Procurement Tecnologie Biomediche

Ing. Barbara Podda
ARES Sardegna – S.C. Governo delle Tecnologie Sanitarie

Avv. Giovanni Battista Gallus
Array Law Studio Legale

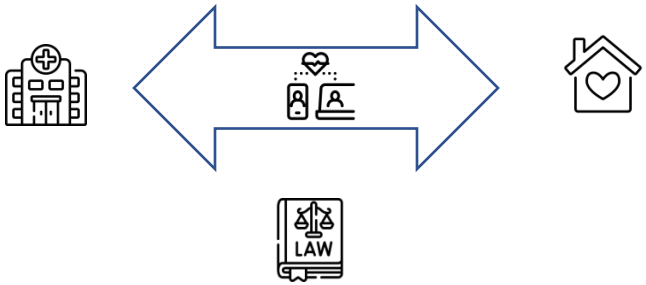
Avv. Giacomo Crovetti
Karanoa SRL

Avv. Salvatorangelo Planta
Karanoa SRL

Ing. Alessio Loberto
ARNAS Brotzu

Descrizione

Necessità di disciplinare nei contratti di fornitura gli aspetti inerenti la titolarità e la responsabilità del trattamento dei dati personali e particolari raccolti e trasmessi dai dispositivi medici con particolare riguardo all'utilizzo di piattaforme telematiche per la trasmissione dei dati.



https://www.flaticon.com/free-icons

Descrizione

Nel contesto del Regolamento Generale sulla Protezione dei Dati (GDPR), i “dati personali” e i “dati particolari” hanno significati specifici:

Dati personali: Secondo l’articolo 4 del GDPR, un dato personale è qualsiasi informazione relativa a una persona fisica identificata o identificabile, direttamente o indirettamente, tramite riferimenti a un identificativo come il nome, un numero di identificazione, dati sulla localizzazione, un identificativo online, o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Dati particolari: I dati particolari, noti anche come “categorie particolari di dati personali” (art. 9 del GDPR), includono dati che rivelano origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, ***dati genetici, dati biometrici, dati sulla salute, vita sessuale o orientamento sessuale***

https://www.flaticon.com/free-icons

Descrizione

Il titolare è il soggetto che, alla luce del concreto contesto nel quale avviene il trattamento, determina le decisioni di fondo relative a finalità e modalità di un trattamento effettuato in base a uno dei presupposti di liceità di cui agli artt. 6 e 9 del Regolamento

La figura del responsabile rimane invece connotata dallo svolgimento di operazioni di trattamento di dati personali delegate dal titolare il quale, all'esito di proprie scelte organizzative, può individuare un soggetto particolarmente qualificato allo svolgimento delle stesse in termini di conoscenze specialistiche, di affidabilità e di risorse per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento

Descrizione

1 Cosa è il registro delle attività di trattamento?

L'art. 30 del Regolamento (EU) n. 679/2016 (di seguito "RGPD") prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento.

E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento (sul registro del responsabile, vedi, in particolare, il punto 6).

Costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Descrizione

La definizione dei ruoli può essere regolata con diverse modalità, ma è fondamentale creare un sistema di governance dei dati individuando i ruoli attraverso una visione complessiva delle operazioni di trattamento che tenga conto delle diverse finalità per le quali i trattamenti sono svolti e dunque delle diverse basi giuridiche sulle quali essi si fondono.

ARES Sardegna, che opera da Centrale di committenza per conto delle Aziende sanitarie della Regione, e per tramite del Dipartimento della Sanità Digitale e dell'Innovazione tecnologica gestisce le attività tecniche, nell'ambito di un processo negoziale, in accordo con i DPO di tutte le Aziende sanitarie regionali, ha dovuto precisare in maniera dettagliata i ruoli in materia di trattamento dei dati tenendo conto del considerando 26 delle Linee guida 7 del 2020 emanate dal Comitato europeo per la protezione dei dati, che recita come segue: ***"La necessità di una valutazione fattuale significa anche che la titolarità di un trattamento non deriva dalle caratteristiche soggettive di chi tratta i dati, ma dalle attività concretamente svolte da tale soggetto in un contesto specifico. In altre parole, uno stesso soggetto può agire contemporaneamente in qualità di titolare del trattamento per determinate operazioni di trattamento, e in qualità di responsabile del trattamento per altre operazioni; inoltre, la qualifica di titolare o di responsabile del trattamento va valutata in relazione a ciascuna specifica attività di trattamento dei dati."***

Descrizione

Parere sullo schema di decreto legislativo, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2017/745, relativo ai dispositivi medici - 26 maggio 2022 [9782450]

IL GARANTE

ai sensi dell'articolo 36, paragrafo 4, del Regolamento, esprime parere favorevole sul proposto schema di decreto legislativo, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2017/745, relativo ai dispositivi medici, con le seguenti condizioni, esposte nel "Ritenuto", volte a suggerire l'opportunità di:

a) introdurre una specifica disposizione sulla protezione dei dati personali trattati nell'ambito delle attività funzionali alla fornitura o manutenzione dei dispositivi, tale da:

- inibire l'accesso ai dati anagrafici e anamnestici del paziente, salva l'indispensabilità ai fini dell'erogazione del servizio di manutenzione e telediagnosi/teleintervento, rendendo comunque tracciabile ogni operazione di intervento/accesso;

- inquadrare quale responsabile del trattamento, ai sensi dell'articolo 28 del Regolamento, la società produttrice del dispositivo medico, per le attività di controllo della funzionalità dell'apparecchiatura anche a distanza svolta per conto del titolare (c.d. servizi di manutenzione e di assistenza);

b) disciplinare, anche nell'ambito dei provvedimenti attuativi cui già lo schema di decreto legislativo rinvia e su cui sarà opportuno acquisire il parere del Garante:

- i tempi di conservazione dei dati personali del fabbricante di dispositivi su misura ai sensi dell'articolo 7;

- i tempi di conservazione dei dati personali eventualmente forniti contestualmente alle comunicazioni di incidenti verificatisi dopo l'immissione in commercio di un dispositivo medico, ai sensi dell'articolo 10, c. 8

Roma, 26 maggio 2022

Descrizione

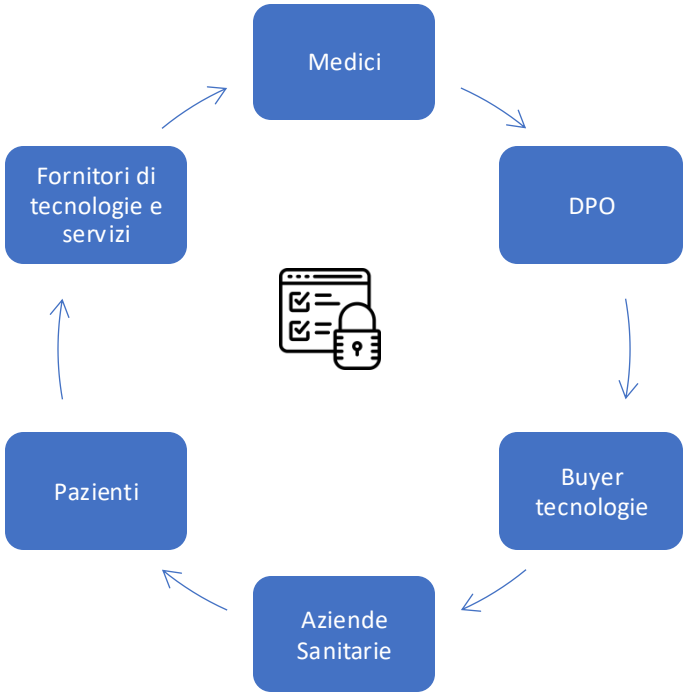
“in relazione ai trattamenti in esame possono verificarsi situazioni in cui uno stesso soggetto (ad esempio il gestore della piattaforma) può assumere il ruolo di titolare per taluni trattamenti che di responsabile per altri trattamenti”.

Obiettivi e destinatari del lavoro

Obiettivi:

Definire ambiti specifici di attività in cui il fornitore di tecnologie e servizi agisce non solo come responsabile del trattamento dei dati, ma come titolare o contitolare degli stessi per attività legate alla sicurezza e alla gestione delle piattaforme telematiche che raccolgono i dati generati da dispositivi medici. In questo caso risulta fondamentale che i contratti di fornitura disciplinino con estrema precisione gli ambiti di competenza in relazione ai diversi ruoli ricoperti per la gestione del dato da parte del fornitore e assicurino, nel contempo, che al paziente venga fornita un'adeguata informativa su tali aspetti e ruoli all'atto della consegna dei dispositivi.

Destinatari:



https://www.flaticon.com/free-icons

Risultati

Fornitore e pubblica amministrazione devono collaborare in modo responsabile e nel rispetto dei principi di correttezza e buona fede in relazione agli obblighi di segnalazione previsti nel GDPR. Per queste motivazioni è bene che il contratto di fornitura venga sempre accompagnato da un apposito accordo sul trattamento dei dati personali (DPA Data Protection Agreement)

Definizione di uno uno schema contrattuale di riferimento applicabile alle differenti tipologie contrattuali in cui vengono forniti servizi connessi ad apparecchiature medicali che comportano il trattamento di dati personali e sensibili degli assistiti approvato da tutti i DPO Aziendali a Marzo del 2024.

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ARES

associazione italiana ingegneri clinici

Risultati

-le Aziende Sanitarie rivestono la qualifica di titolari per le attività di trattamento dei dati relativi allo stato di salute dei pazienti generati dal dispositivo.

-per le attività di assistenza e terapia sanitaria ai sensi dell'art. 9, par. 2 lett. h) del Regolamento, il Fornitore, nella sua qualità soggetto particolarmente qualificato, in virtù delle sue conoscenze specialistiche, verrà designato dalle Aziende Sanitarie quale Responsabile del trattamento ai sensi dell'art. 28 del Regolamento 2016/679, in conformità anche a quanto previsto, in materia di dispositivi medici, dall'art. 21, comma 3 del D.Lgs. 5 agosto 2022, n. 137, ai sensi del quale "Qualora per il dispositivo medico siano previste dal fabbricante attività di taratura, calibrazione, manutenzione o assistenza, da svolgersi anche a distanza, il responsabile del trattamento ai sensi dell'articolo 28 del regolamento (UE) 2016/679 è il fabbricante del dispositivo medico."

-il fornitore, quale proprietario e gestore della piattaforma telematica, rivestirà il ruolo di titolare autonomo del trattamento solo ed esclusivamente con riferimento al trattamento dei dati necessari per finalità di natura tecnica correlate alla sicurezza e gestione dei prodotti e servizi offerti, e comunque nel rispetto di una base giuridica del trattamento consentita dall'art. 9 del GDPR e in relazione a tali attività il fornitore si baserà, in ogni misura possibile, su dati anonimizzati, aggregati e/o de-identificati, in conformità al principio unionale e nazionale sulla minimizzazione dei dati;

-le aziende sanitarie e il fornitore dovranno fornire al paziente un'adeguata informativa, rappresentando correttamente agli interessati i rispettivi ruoli e le modalità del trattamento all'atto della consegna dei dispositivi, ciò anche al fine di consentire l'eventuale esercizio dei diritti che il GDPR riconosce agli interessati.

AIIC 2024 AWARDS

ARES Sardegna

Dipartimento Sanità Digitale e Innovazione Tecnologica ARES Sardegna

Dott. Giovanni Scarteddu
giovanni.scarteddu@aressardegna.it
Responsabile S.S. Procuremente Tecnologie Biomediche

Ing. Barbara Podda
Direttrice S.C. Governo delle Tecnologie Sanitarie
barbara.podda@aressardegna.it

AIIC associazione italiana ingegneri clinici