CONVEGNO

La Regolamentazione della protezione dei dati personali nell'ambito della medicina sportiva

NUOVE TECNOLOGIE, DISPOSITIVI MEDICI, IOT: PROFILI SPECIFICI PRIVACY

Avv. Silvia Stefanelli

ORGANIZZATO DA

CON IL PATROCINIO DI

07 GIUGNO 2023

casistica

dispositivi di monitoraggio continuo dei valori del fitness

app e smartwact intelligenti per l'alimentazione, il sonno e l'attività fisica

occhiali con display per leggere i dati di velocità e distanza

scarpe con sensori

caschi con GPS integrato

activity Tracker indossabili utili alla raccolta di dati sullo stile di vita

elettrocardiografi

spirometri

defribrillatori

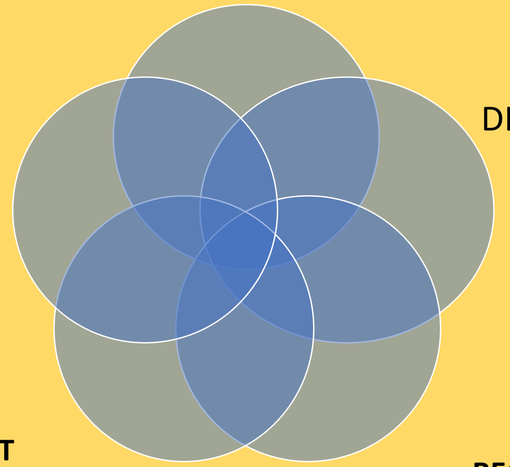
holder ECG e pressorio

la «filiera» (del rischio)

- soggetti che progettano il software
- produttori componenti
- soggetti che immettono sul mercato
- soggetti che importano dall’estero
- soggetti distribuiscono sul territorio comunitario
- piattaforme raccolta dati
- fornitori di connettività
- strutture sanitarie che raccolgono i dati (IOT o tramite telemedicina)

DISCIPLINE ORIZZONTALI

GDPR



Cyber Resilience Act

DIRETTIVA NIS (2)

CYBERSECURITY ACT

PROPOSTA REGOLAMENTO AI

DISCIPLINE VERTICALI

DISPOSITIVI MEDICI

REG. 2017/745

I TEMI PRIVACY

LA DEFINZIONE DEI RUOLI PRIVACY

L’ AMPIA RACCOLTA DI DATI (big data)

LE BASI GIURIDICHE

LA CYBERSECURITY

LA DEFINZIONE DEI RUOLI PRIVACY

I PROCESSI DI TRATTAMENTO POSSONO ESSERE NUMEROSI

I SOGGETTI COINVOLTI POSSONO ESSERE NUMEROSI

disegno dei processi
determinazione delle finalità
definizione dei ruoli

BIG DATA

…il GDPR non è stato pensato per i Big Data…

INDAGINE CONOSCITIVA SUI BIG DATA
Garante privacy e AGCM e AGCOM
10 febbraio 2020

…Il GDPR, anche se non si occupa direttamente di Big Data, prevede disposizioni applicabili a tali ipotesi, volte a fronteggiare i potenziali rischi derivanti dalla profilazione e dal processo decisionale automatizzato e a tutelare i diritti fondamentali degli interessati, ponendo limitazioni nei casi in cui i Big Data possano avere un impatto significativo sugli individui (pag. 56)…

BIG DATA

la profilazione (art. 22)

la valutazione d’impatto (art. 35)

LE BASI GIURIDICHE

WP29 5 febbraio 2015
Nozione di dato sanitario

…….i dati generati da dispositivi o applicazioni, che vengono utilizzati in contesto medico, indipendentemente dal fatto che i dispositivi siano qualificati come "dispositivi medici"…..

LE BASI GIURIDICHE

DATI PERSONALI

IL CONTRATTO

IL CONSENSO

(*marketing)*

L'INTERESSE LEGITTIMO

(*miglioramento software*)

DATI RELATIVI ALLA SALUTE

IL CONSENSO (art. 9 lett. a)

FINALITA' DIAGNOSI E CURA (art. 9 lett. h)

e lo stretto collegamento con l'informativa
INFORMATIVA

LA CYBERSECURITY

2018 – militare con dispositivo indossabile STRAVA dotato di GPS,
ha portato ad individuare una base militare
doveva rimanere segreta
“Fitness tracking app Strava gives away location of secret US army bases” su
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

2018 – incidente MyFitnesspal
150 milioni di dati - offerti sul dark web

https://fortune.com/2019/02/14/hacked-myfitnesspal-data-sale-dark-web-one-year-breach/

LA CYBERSECURITY

Proposta regolamento cybersecurity act

DISPOSITIVI MEDICI

REG. 2017/745

CYBERSECURITY
DISPOSITIVI MEDICI

dir 93/42/CEE sui dm

dir 2007/47/CEE

Nessuna disciplina specifica per i software

CYBERSECURITY
DISPOSITIVI MEDICI

Reg. UE 2027/745

ampliamento dei software che vengono classificati come DM

disciplina molto dettagliata per i software

CYBERSECURITY
DISPOSITIVI MEDICI

AMPLIAMENTO CASISTICA

ALLEGATO VIII regola 11

Il software destinato a fornire informazioni utilizzate per prendere decisioni a fini diagnostici o terapeutici *è classificato* ***nella classe IIa,***

tranne se tali decisioni hanno un impatto che può causare:

- *morte o un deterioramento irreversibile dello stato di salute di una persona, nel qual caso è* ***in classe III****; oppure*
- *un grave deterioramento dello stato di salute di una persona o un intervento chirurgico, nel qual caso è classificato come* ***classe IIb.***

è SAMD il software fornisce
informazioni che servono a prendere decisioni terapeutiche

CYBERSECURITY
DISPOSITIVI MEDICI

ALLEGATO I

i requisiti specifici per il software

17.2. Per i dispositivi contenenti un software o per i software che costituiscono dispositivi a sé stanti, il software è ***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.*

SICUREZZA INFORMAZIONI

CYBERSECURITY
DISPOSITIVI MEDICI

ALLEGATO I

i requisiti specifici per il software

17.3. I software di cui al presente punto destinati a essere usati in combinazione con piattaforme di calcolo mobili sono progettati e fabbricati tenendo conto delle peculiarità della piattaforma mobile (ad esempio dimensioni e grado di contrasto dello schermo) e di fattori esterni connessi al loro uso (variazioni ambientali relative al livello di luce o di rumore).

17.4. ***I fabbricanti indicano 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.***

USABILITA'

CYBERSECURITY –
la carenza non permette di apporre la marcatura CE

CYBERSECURITY
DISPOSITIVI MEDICI

MDCG 2019-16

Guidance on Cybersecurity for medical devices

December 2019

CYBERSECURITY

PROPOSTA CYBER RESILIENCE ACY

DISCIPLINA SUI SOFTWARE GENERICI

……ad oggi nessuna disciplina specifica…..

CYBERSECURITY

PROPOSTA CYBER RESILIENCE ACY

COMMISSIONE
EUROPEA

Bruxelles, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020

(Testo rilevante ai fini del SEE)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

CYBERSECURITY

PROPOSTA CYBER RESILIENCE ACY

Sebbene la normativa vigente in materia di mercato interno si applichi ad alcuni prodotti con elementi digitali, la maggior parte dei prodotti hardware e software non è attualmente disciplinata da alcuna normativa dell'UE riguardante la loro cybersicurezza.

In particolare l'attuale quadro giuridico dell'UE non affronta la questione della cybersicurezza del software non incorporato, anche se gli attacchi alla cybersicurezza prendono sempre più di mira le vulnerabilità di tali prodotti, causando costi sociali ed economici significativi

CYBERSECURITY

PROPOSTA CYBER RESILIENCE ACY

2 OBIETTIVI PRINCIPALI

creare le condizioni per lo sviluppo di prodotti con elementi digitali sicuri, garantendo che i prodotti hardware e software siano immessi sul mercato con un minor numero di vulnerabilità, e far sì che i fabbricanti prendano la sicurezza in seria considerazione durante l'intero ciclo di vita di un prodotto;

creare le condizioni che consentano agli utilizzatori di tenere conto della cybersicurezza nella scelta e nell'utilizzo dei prodotti con elementi digitali.

4 OBIETTIVI SPECIFICI

- garantire che i fabbricanti migliorino la sicurezza dei prodotti con elementi digitali fin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita;
- garantire un quadro coerente in materia di cybersicurezza, facilitando la conformità per i produttori di hardware e software;
- migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali e;
- consentire alle imprese e ai consumatori di utilizzarli in modo sicuro.

CYBERSECURITY

PROPOSTA CYBER RESILIENCE ACY

LA PROPOSTA DI REGOLAMENTO
RIENTRA NELLA FAMIGLIA DELLE DISCIPLINE

NEW LEGISLATIVE FRAMEWORK (2008)

quindi prodotti marcati CE

CYBERSECURITY

PROPOSTA CYBER RESILIENCE ACY

OGGETTO

a) **norme per l'immissione sul mercato di prodotti** con elementi digitali per garantire la cybersicurezza di tali prodotti;

b) **requisiti essenziali per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali** e **obblighi per gli operatori economici in relazione a tali prodotti per quanto riguarda la cybersicurezza**;

c) **requisiti essenziali per i processi di gestione delle vulnerabilità** messi in atto dai fabbricanti per garantire la cybersicurezza dei prodotti con elementi digitali durante l'intero ciclo di vita e obblighi per gli operatori economici in relazione a tali processi;

d) **norme sulla vigilanza del mercato** e sull'applicazione delle norme e dei requisiti di cui sopra.

proposta di regolamento sull' AI

COMMISSIONE
EUROPEA

Bruxelles, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (LEGGE SULL'INTELLIGENZA ARTIFICIALE) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE

requisiti etici da rispettare

controllo di un organismo notificato

apposizione di una marcatura CE

sorveglianza post commercializzazione

LE RISORSE ONLINE:

www.studiolegalestefanelli.it

https://privacygdpr.it/

https://www.medicaldevicenews.eu/

Osservatorio europeo della privacy

Osservatorio sanzioni privacy

Rubrica ricerca scientifica e privacy

Raccolta fonti normative sull'Intelligenza Artificiale

Rubrica DM tra normativa e regolatorio con Aboutpharma

Osservatorio europeo DM

Grazie dell’attenzione!

Avv. Silvia Stefanelli

s.stefanelli@studiolegalestefanelli.it

ORGANIZZATO DA

CON IL PATROCINIO DI