EHDS & Cybersecurity – Implicazioni legali per il settore sanitario

e-privacy XXXVI (2025): ***La vita è tutto un dossier***

Relatore: Avv. Filippo Bianchini

Chi sono

- Avvocato cassazionista, iscritto al Foro di Perugia
- DPO e Valutatore privacy certificato UNI 11697 – Lead Auditor 27001:2022 – CIPP/E
- Membro supplente dell'Autorità Garante per la protezione dei dati personali di San Marino
- Componente del Consiglio Direttivo di ASSO DPO e di AIP-ITCS, nonché del Comitato Scientifico di Clusit
- Docente nel Master Universitario Data Protection, Cybersecurity e Digital Forensicsdell'Università degli Studi di Perugia e nel progetto Erasmus+ BuTH-AI, Building Trust In Human-Centric Artificial Intelligence della Link Campus University
- Membro dell'EDPB «Support Pool of Experts»
- Membro del Cybersecurity National Lab, nodo UniPg
- Componente UNI CT 510

Cos'è l'EHDS

Regolamento (UE) 2025/327

Istituisce lo Spazio Europeo dei Dati Sanitari (European Health Data Space).

Quadro comune UE

Definisce regole per il trattamento, lo scambio e il riutilizzo dei dati sanitari elettronici.

Integrazione normativa

Si coordina con GDPR, NIS2 e Data Governance Act in un ecosistema regolamentare coerente.

Cronologia & Entrata in vigore

3 maggio 2022

Proposta della Commissione Europea

15 marzo 2024

Accordo provvisorio Consiglio-Parlamento

24 aprile 2024

Adozione del Parlamento Europeo

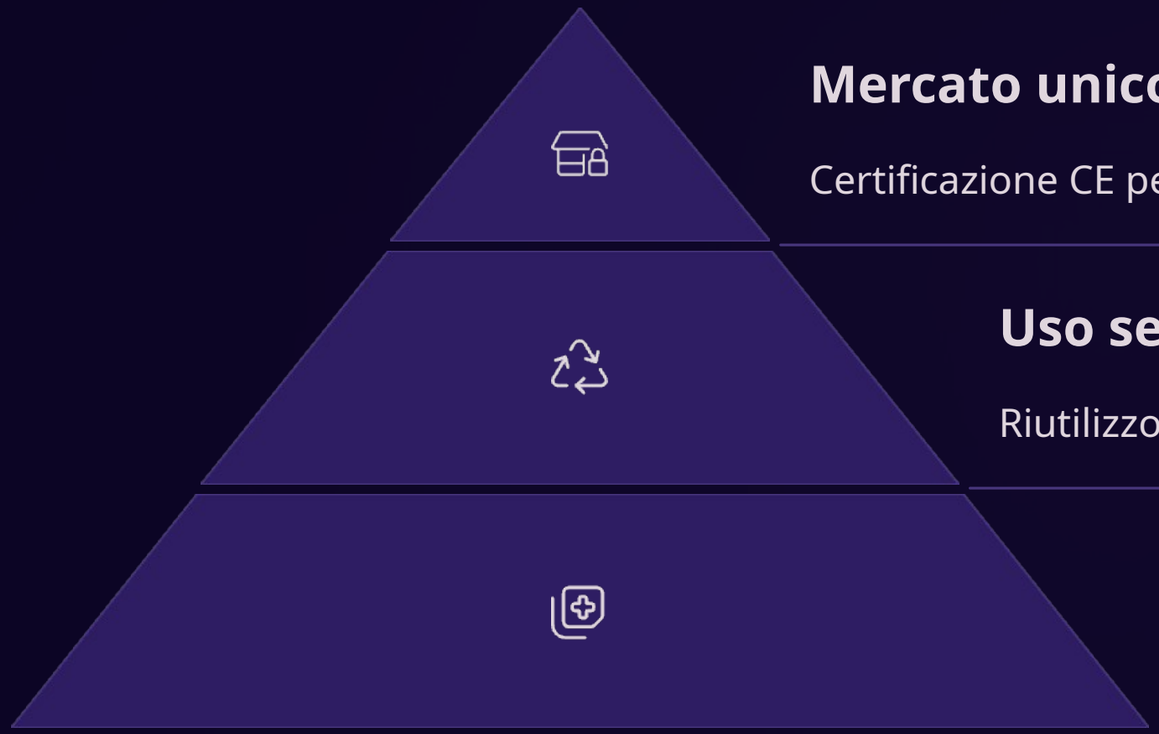
6 marzo 2025

Pubblicazione nella Gazzetta Ufficiale dell'UE

26 marzo 2025

Entrata in vigore del Regolamento

Pilastri principali



Mercato unico

Certificazione CE per EHR e servizi digital health

Uso secondario

Riutilizzo sicuro dei dati tramite HealthData@EU

Uso primario

Accesso transfrontaliero ai dati con MyHealth@EU

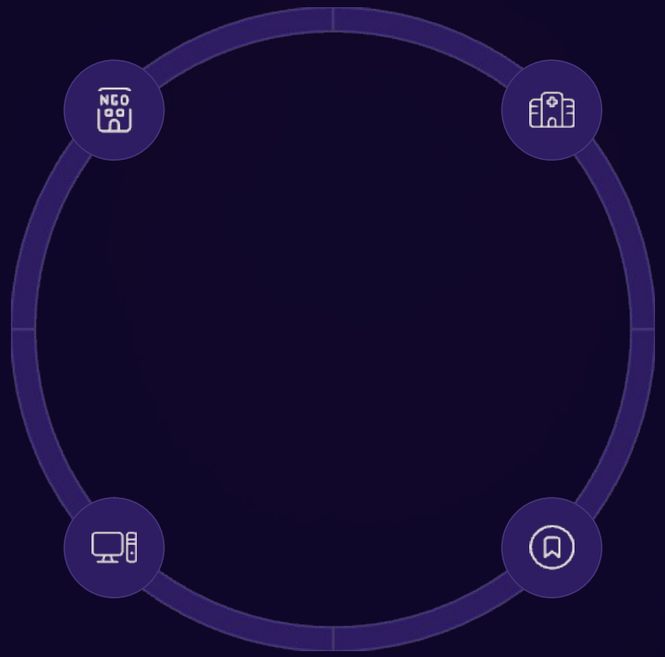
Attori & Governance

Health Data Access Bodies

Autorità nazionali che autorizzano il riutilizzo dei dati sanitari.

Fornitori EHR/mHealth

Soggetti obbligati alla certificazione dei sistemi.



Data Holders

Strutture sanitarie, laboratori e farmacie che detengono i dati.

Data Users

Ricercatori, industria life-sciences e autorità pubbliche.

Diritti degli interessati

Accesso immediato

Diritto di accedere gratuitamente ai propri dati sanitari elettronici.

Rettifica e integrazione

Possibilità di correggere o completare i propri dati sanitari.

Opt-out

Diritto di opposizione all'uso secondario, con eccezioni per salute pubblica.

Portabilità transfrontaliera

Accesso ai propri dati tramite formato europeo comune (EHRxF-EU).

Obblighi per operatori sanitari & fornitori IT

Interoperabilità

Adozione di standard comuni: HL7-FHIR, SNOMED-CT, ICD-10, LOINC.

Certificazione

Marcatura CE obbligatoria per sistemi EHR e AI ad alto rischio.

Protezione dati

Pseudonimizzazione e minimizzazione per uso secondario dei dati.

Valutazione impatto

DPIA integrati con assessment specifici per EHDS.

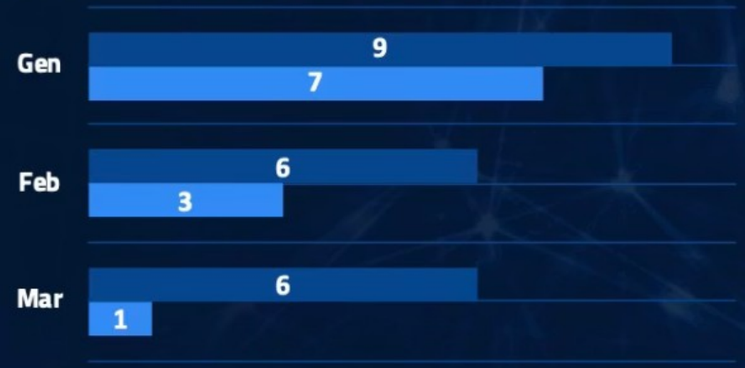
Il settore a colpo d'occhio

EVENTI CYBER E INCIDENTI (2023-2024)

Trend eventi cyber e incidenti dal 2023 al 2024

- Eventi cyber registrati nel 2024
- Incidenti registrati nel 2024
- Media mensile eventi cyber nel 2023
- Media mensile incidenti nel 2023

EVENTI CYBER E INCIDENTI (2025)



Trend eventi cyber e incidenti nel 2025

- Eventi cyber registrati nel 2025
- Incidenti registrati nel 2025

PRINCIPALI IMPATTI SUI SOGGETTI

- BLOCCO TEMPORANEO DI SERVIZI
- ESFILTRAZIONE DI DATI
- MODIFICHE ALL'INTEGRITÀ

Minaccia prevalente: **Ransomware**

VULNERABILITÀ ESPOSTE

IP monitorati che presentano criticità:

CONFIGURAZIONI ERRATE CHE NON RISPETTANO BEST PRACTICE — 57%

DISPOSITIVI E SERVIZI ESPOSTI INCAUTAMENTE — 31%

SERVIZI CON VULNERABILITÀ O OBSOLETI — 12%

PRINCIPALI CAUSE DELLE BAD PRACTICES

GESTIONE DECENTRALIZZATA

Diversi reparti ottengono hardware, software e servizi IT da fornitori esterni senza una gestione centralizzata.

CARENZA DI PERSONALE DEDICATO A CYBERSICUREZZA

Il personale IT gestisce la sicurezza informatica senza avere risorse dedicate, facendo al meglio delle proprie possibilità.

OBSOLESCENZA DEI DISPOSITIVI

Apparati informatici obsoleti, non aggiornabili o supportati, che continuano ad essere utilizzati.

Impatto sull'ecosistema cybersecurity

Espansione superficie d'attacco

L'interconnessione dei sistemi richiede l'implementazione di architetture Zero Trust.

Security-by-design

I sistemi EHR certificati devono incorporare la sicurezza fin dalla progettazione.

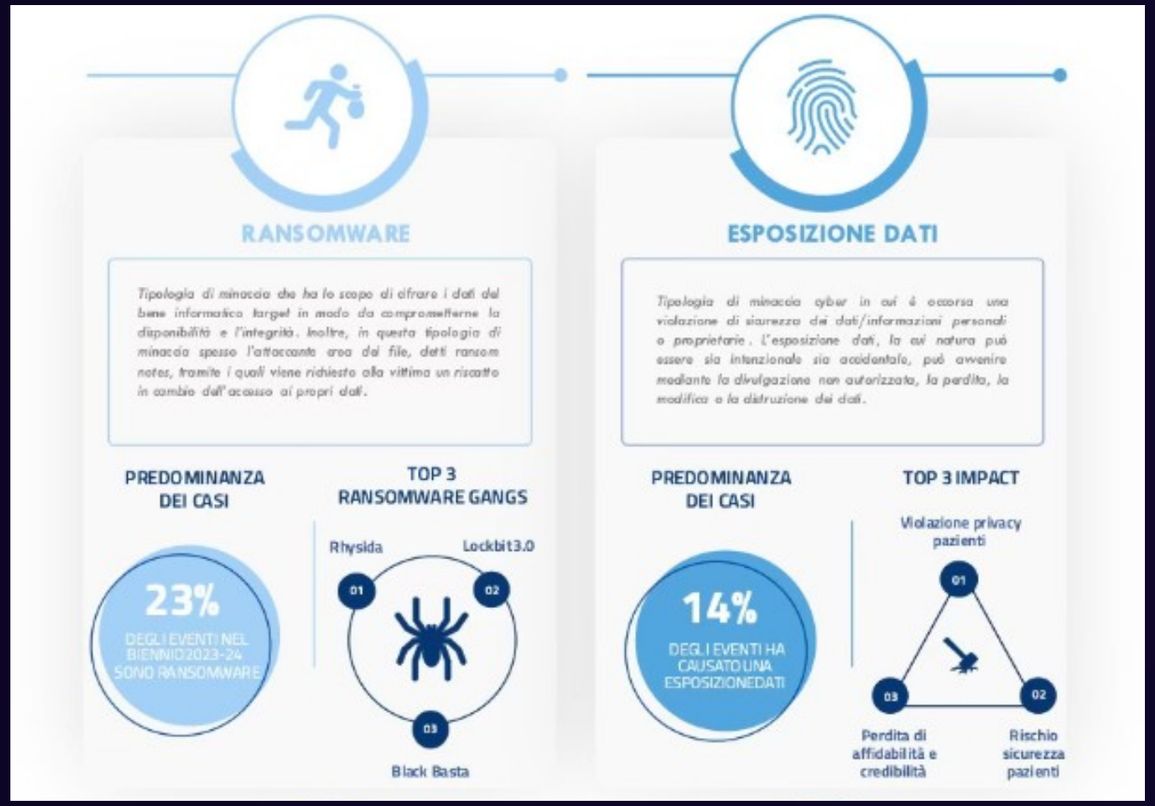
Verifica continua

Audit periodici e penetration test diventano obbligatori per garantire la sicurezza.

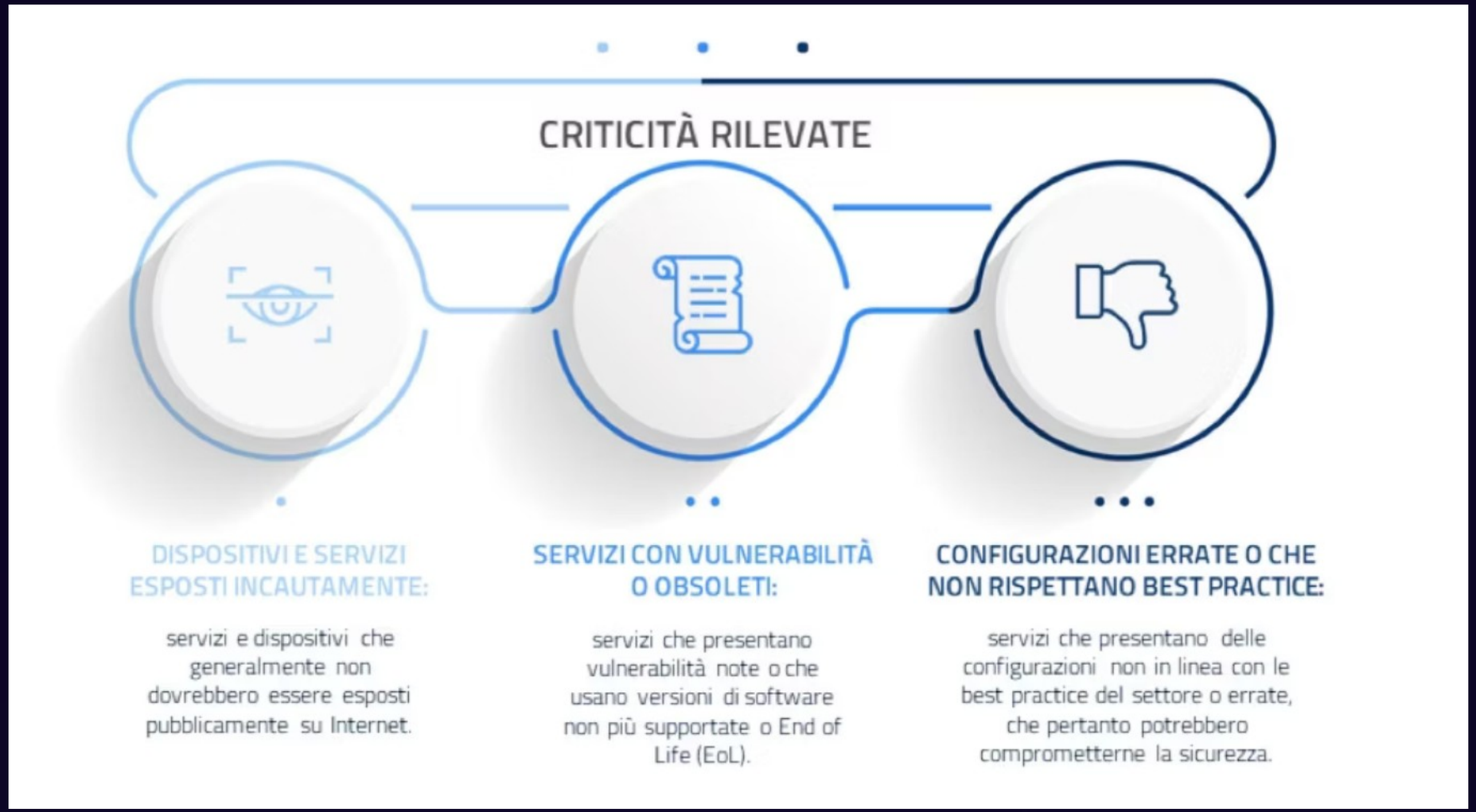
Monitoraggio integrato

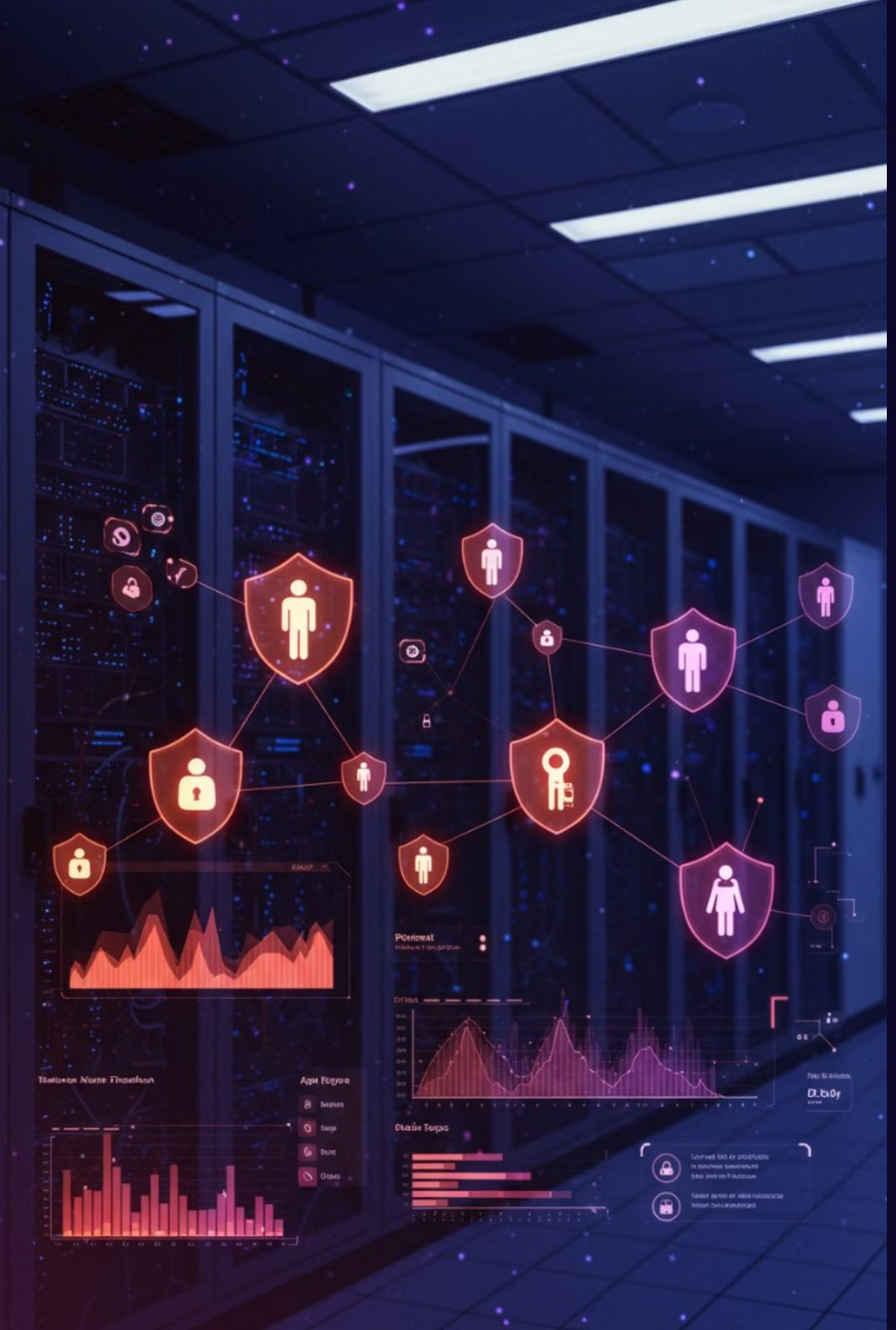
I log di sistema devono integrarsi con CSIRT nazionale e HealthData@EU.

La minaccia cyber al settore sanitario



Classificazione delle criticità rilevate nel settore sanitario





EHDS & Resilienza cyber – Requisiti chiave

Misure adeguate

Art. 39 EHDS impone misure tecniche e organizzative per la protezione dei dati.

Allineamento NIS2

Conformità alle norme sui servizi essenziali nel settore sanitario.

Incident reporting

Notifica obbligatoria entro 24 ore a CSIRT nazionale e HDAB.

Verifica indipendente

Audit obbligatori per tutti i sistemi EHR certificati.

Strategia di compliance integrata

Mappatura flussi dati

Inventario completo degli asset informativi

Aggiornamento DPIA

Analisi rischi integrata cyber-EHDS

Contrattualistica fornitori

SCC con clausole EHDS specifiche

Crittografia end-to-end

Tokenizzazione dati sensibili

Formazione continua

Aggiornamento personale clinico/IT

Opportunità per ricerca & policy

Sviluppo AI e medicina di precisione

L'EHDS offre dataset pseudonimizzati per sviluppare AI e medicina di precisione.

Federated learning e privacy

Il federated learning garantisce analisi rispettose della privacy sui dati sanitari.

Partenariati per l'innovazione

Sandbox regolamentari favoriscono i partenariati pubblico-privato per l'innovazione.

Le raccomandazioni più rilevanti per il settore

Grazie per l'attenzione!

Domande?

Avv. Filippo Bianchini

(+39) 3492864103

info@bianchini.legal

LinkedIn: studiolegale