DECISIO – Privacy & Cyber Security Overview

Modello di Governance, Compliance GDPR e Misure di Sicurezza

Dr.ssa Francesca Ronzoni, **DPO**
ID 7201D3D8/2022

Executive Summary

Piattaforma software medicale progettata secondo i principi di Privacy by Design, conforme al Regolamento (UE) 2016/679 (GDPR).

Ruoli GDPR

Net Medicare opera come Responsabile del Trattamento (Processor); il Cliente è Titolare (Controller).

Data Residency

Hosting esclusivo in UE/SEE

Sicurezza

Cifratura end-to-end (AES-256 at rest, TLS 1.2+ in transit) e autenticazione forte (MFA).

AI Governance

Moduli AI a inferenza privata. Nessun addestramento (training) sui dati dei pazienti.

Access Control

Gestione accessi granulare (RBAC) e autenticazione MFA nativa.

Deployment

Disponibile in modalità SaaS multi-tenant o On-Premise single tenant.

Governance Privacy e Compliance (GDPR)

Ruoli e Responsabilità (Art. 28)

Nomina formale di Net Medicare a Responsabile.

Supporto al Titolare nella gestione dei diritti degli interessati (Artt. 15-22).

Accountability (Art. 30 & 35)

Registro dei Trattamenti mantenuto e aggiornato.

DPIA (Valutazione d'Impatto) eseguita per AI e dati su larga scala.

Rischio residuo: Accettabile.

Audit e Verifiche

Legal Opinion indipendente conferma la conformità.

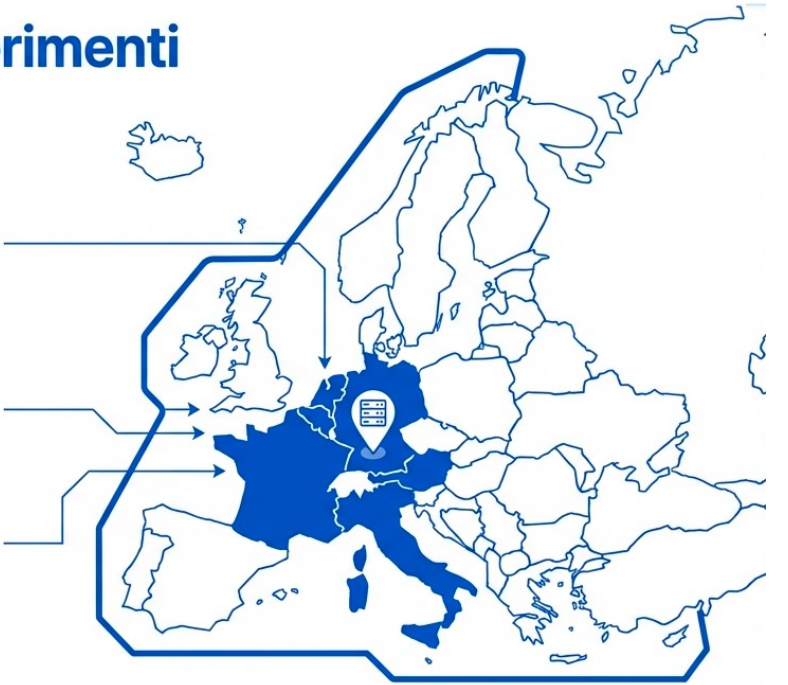
Nomina del DPO (Data Protection Officer) e Security Officer interni.

Data Residency e Trasferimenti

Hosting Primario
Infrastruttura situata in UE

Politica di Trasferimento
Nessun trasferimento di dati personali
al di fuori dello Spazio Economico Europeo

Supply Chain (Sub-responsabili)
vincolata da contratti (DPA) che impongono i medesimi obblighi di sicurezza.



Misure di Sicurezza: Protezione e Accesso (Art. 32 GDPR)

Cifratura (Encryption)

At-rest: Database e backup cifrati AES-256.
In-transit: Traffico HTTPS (RSA 2048) e TLS 1.2+.

Identity & Access (IAM)

RBAC (Role-Based Access Control) con principio di Least Privilege. Supporto nativo per MFA (2FA).

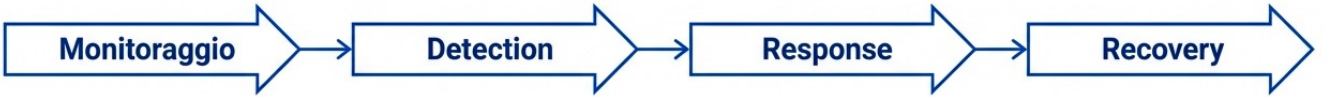
Segregazione Tenant

Isolamento logico rigoroso tramite Tenant ID e separazione a livello applicativo/database.

Procedura Break-Glass

Accesso supporto tecnico consentito solo su ticket, Just-In-Time (temporaneo) e interamente tracciato.

Misure di Sicurezza: Monitoraggio e Resilienza



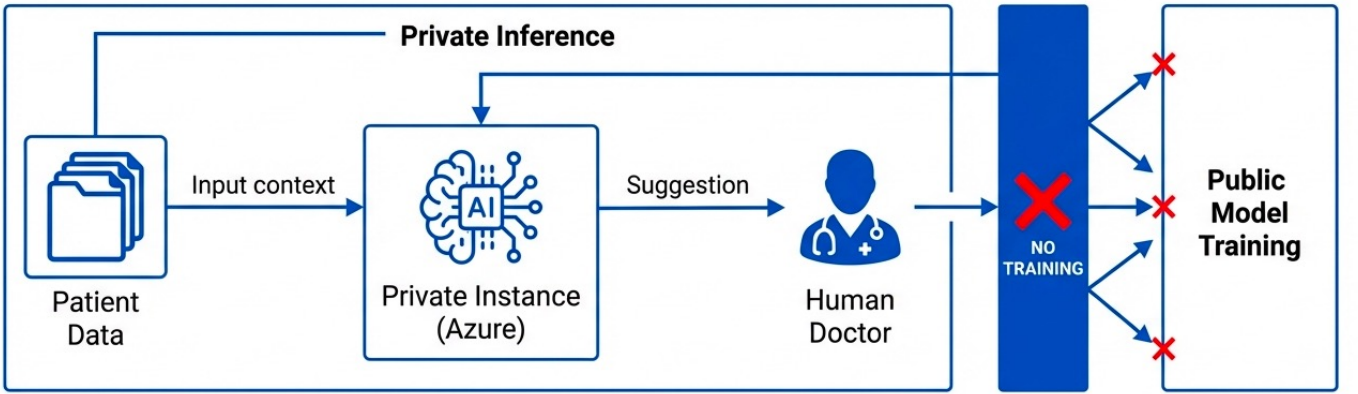
Audit Logging:
Tracciamento immutabile delle operazioni critiche (login, consultazione, export). Retention log per finalità forensi (12-24 mesi).

Vulnerability Management:
Scansioni periodiche e Penetration Test annuali (o a major release). Gestione patch centralizzata.

Business Continuity & DR:
Backup giornalieri cifrati e ridondati. Test periodici di ripristino (Restore test) per verificare l'integrità.

Incident Response:
Procedura formalizzata di gestione Data Breach con notifica al Titolare entro i termini di legge (<24h).

AI Governance & Sicurezza



Zero Training: I dati dei pazienti NON vengono utilizzati per **l'addestramento** dei modelli.

Human-in-the-Loop: L'AI è un supporto (CDSS). Nessuna decisione automatizzata (No Art. 22 GDPR). L'output richiede sempre validazione umana.

Technology: Modelli LLM (es. GPT-4o) in istanza privata.

Modello di Responsabilità Condivisa (Shared Responsibility)

Ambito	SaaS (Cloud)	On-Premise
Gestione Utenti (IAM)	Condiviso	Condiviso
Patching Applicativo	**DECISIO**	**DECISIO**
Patching OS / DB	**DECISIO**	Cliente
Backup Dati	**DECISIO**	Cliente
Sicurezza Fisica	Cloud Provider (Azure)	Cliente
Logging	**DECISIO** (generazione)	Cliente (monitoraggio)
Incident Response	Cooperazione	Titolare (con supporto)

In modalità On-Premise è vietato al Cliente modificare componenti applicativi senza autorizzazione