Compliance

Mappare gli obblighi di conformità che gravano sul Fondo / Cassa quando attiva servizi di digital health

I sette domini di compliance

Il Fondo resta Titolare e accountable — non si delega al provider

PRIVACY

GDPR · D.lgs 196/2003

Il Fondo deve identificare le basi giuridiche per ogni trattamento di dati, tenere un registro aggiornato, redigere le informative agli iscritti, nominare il provider come responsabile e gestire tempestivamente le violazioni dei dati.

SANITARIA

Accordo Stato-Regioni 2020

Le prestazioni di telemedicina erogate dal Fondo devono essere correttamente qualificate nelle quattro categorie ministeriali. I professionisti coinvolti devono avere i titoli richiesti e operare nel rispetto delle linee guida cliniche applicabili.

DISPOSITIVI MEDICI

Reg. UE 2017/745 MDR

Ogni software con finalità clinica — dai sistemi di triage automatizzato alle app di monitoraggio — deve avere la marcatura CE come dispositivo medico (SaMD). Il Fondo non può rimborsare o promuovere strumenti non certificati come dispositivi medici quando la funzione lo richiederebbe.

INTELLIGENZA ARTIFICIALE

AI Act — Reg. UE 2024/1689

I sistemi di IA utilizzati per il triage, la stratificazione del rischio o il supporto diagnostico rientrano probabilmente nella categoria ad alto rischio dell'AI Act. Il Fondo è tenuto a verificare che siano documentati, supervisionati da un operatore umano e conformi ai requisiti di trasparenza.

FISCALE

Art. 51 e 10 TUIR

La corretta distinzione tra prestazioni vincolate (che incidono sul calcolo del 20% deducibile) e non vincolate è condizione per la deducibilità fiscale dei contributi. Errori di classificazione nell'Anagrafe Fondi espongono il Fondo a contestazioni da parte dell'Amministrazione finanziaria.

ASSICURATIVA

Codice delle Assicurazioni

Quando il Fondo eroga servizi di Digital Health attraverso una polizza collettiva o con riassicurazione, le prestazioni digitali devono essere esplicitamente incluse nel perimetro contrattuale con l'assicuratore, con adeguata copertura per la responsabilità civile professionale.

CYBERSECURITY

NIS2 — D.lgs 138/2024

I Fondi che trattano dati sanitari in modo sistematico possono rientrare nell'ambito applicativo della direttiva NIS2. In ogni caso, il contratto con il provider deve includere obblighi di sicurezza informatica, gestione degli incidenti e verifica della supply chain tecnologica.

SPECIFICITÀ PER LA SANITÀ INTEGRATIVA

Il Fondo conserva la responsabilità di titolare del trattamento e di committente accountable indipendentemente dall'affidamento operativo al provider. L'errore più frequente consiste nel trasferire implicitamente la governance della compliance al fornitore. Il presidio deve essere attivo su tutti i sette domini: un inadempimento del provider — in materia di sicurezza, classificazione dei dispositivi medici o disciplina fiscale — produce conseguenze che ricadono sul Fondo.

RIFERIMENTI NORMATIVI

GDPR 2016/679 · MDR 2017/745 · AI Act 2024 · EHDS 2025 · NIS2 2024 · Garante Privacy

DOMANDE APERTE AL TAVOLO

1. Quale presidio interno minimo deve garantire il Fondo per la compliance in ambito digital health? Il DPO è sufficiente o è necessaria una figura di compliance officer dedicata?
2. Definire una checklist di conformità da compilare preventivamente all'attivazione di ogni nuovo servizio digitale: il tavolo può contribuire alla sua redazione?