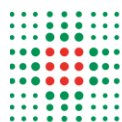


Informazioni generali

- **Titolo:** DPIA Madre Ricerca e Sperimentazione Clinica
- **Titolare del trattamento:** IRCCS Azienda Ospedaliero-Universitaria di Bologna Policlinico di Sant'Orsola
- **Data di avvio della revisione del documento:** 19/02/2026
- **Data di validazione/emissione:** 09/06/2026
- **Parere del DPO:** favorevole (rilasciato nell'ambito dell'approvazione della DPIA) in data 06/07/2026 (nota PG0028295_2026)
- **DPO coinvolto:** Manuel Ottaviano
- **Data prevista per il riesame:** 09/06/2029
- **Periodicità di revisione:** triennale o anticipata in caso di modifiche normative, organizzative o tecnologiche rilevanti.

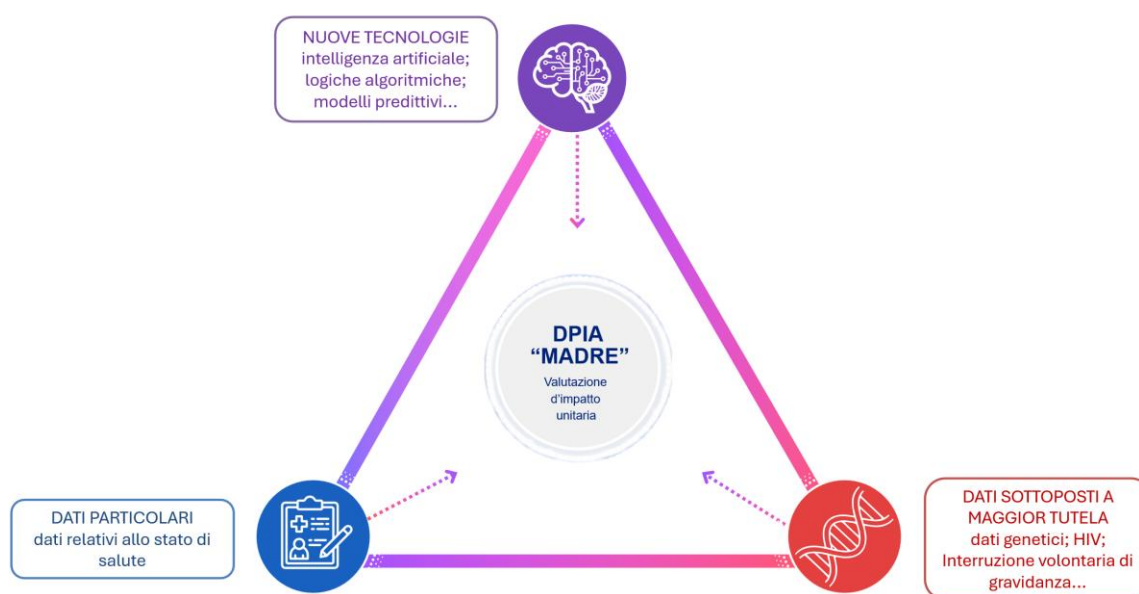
Il presente documento costituisce un estratto informativo della **DPIA Madre "Ricerca e Sperimentazione Clinica"**, elaborata dalle Aziende sanitarie dell'Area Vasta Emilia Centro (AVEC) quale modello di riferimento per la valutazione dei trattamenti di dati personali effettuati nell'ambito della ricerca scientifica e della sperimentazione clinica. La versione integrale della DPIA non è pubblicata per ragioni di sicurezza e per la tutela delle misure tecniche e organizzative adottate dai titolari del trattamento.

L'abstract ha la finalità di illustrare in forma sintetica l'ambito di applicazione del modello, i principali presupposti normativi, le categorie di dati trattati, le tipologie di rischio considerate e le misure generali adottate per garantire la protezione dei dati personali e il rispetto della normativa vigente.



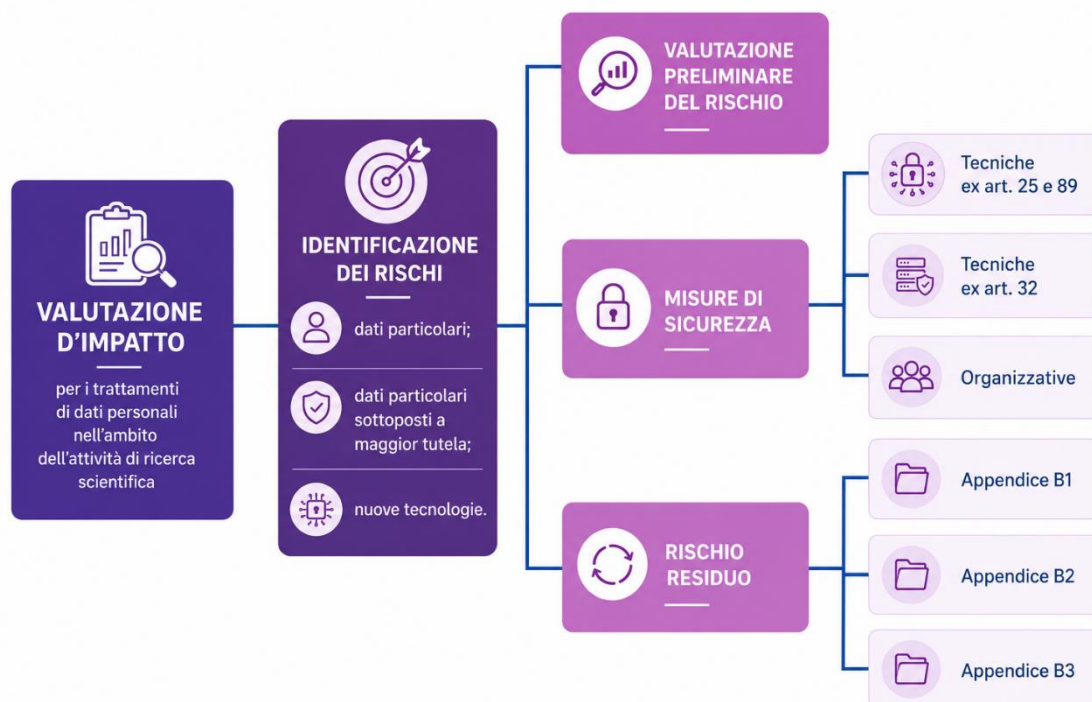
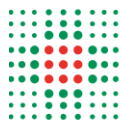
DPIA MADRE

Valutazione d'impatto unitaria dei trattamenti di ricerca medica, biomedica ed epidemiologica



Il documento si applica ai trattamenti effettuati per finalità di ricerca medica, biomedica ed epidemiologica e alle attività amministrative connesse, distinguendo tre principali categorie di trattamenti: **dati particolari**, **dati particolari sottoposti a maggiore tutela** (quali dati genetici, HIV, IVG e informazioni sulla vita sessuale) e **dati trattati mediante nuove tecnologie**, inclusi sistemi di intelligenza artificiale e logiche algoritmiche. Tale approccio consente di analizzare gruppi di trattamenti caratterizzati da rischi omogenei e di adottare misure proporzionate alle specificità di ciascun contesto.

La DPIA evidenzia come la ricerca sanitaria richieda un delicato bilanciamento tra l'interesse pubblico al progresso scientifico e la tutela della riservatezza dei soggetti coinvolti. A tal fine richiama il quadro normativo europeo e nazionale, con particolare riferimento agli artt. 9, 25, 32, 35 e 89 del Reg. UE 2016/679, agli artt. 110 e 110-bis del D.Lgs. 196/2003 e alle disposizioni specifiche applicabili alla ricerca scientifica, ai dati genetici e all'utilizzo dell'intelligenza artificiale.



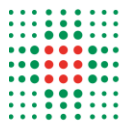
L'analisi dei rischi identifica, tra i principali scenari, la perdita di riservatezza, integrità e disponibilità dei dati, il rischio di reidentificazione degli interessati, la discriminazione derivante dal trattamento di categorie di dati particolarmente sensibili, la gestione degli incidental findings, nonché i rischi connessi all'utilizzo di sistemi di intelligenza artificiale e di tecnologie innovative. La valutazione distingue tre macro-categorie di trattamenti, ciascuna caratterizzata da specifici profili di rischio e da un differente livello di misure di protezione.

Trattamenti aventi ad oggetto dati sanitari e altri dati particolari.

Per tali trattamenti la DPIA individua un sistema di misure tecniche e organizzative volto a garantire la riservatezza, l'integrità e la disponibilità delle informazioni, attraverso l'applicazione dei principi di privacy by design e privacy by default. Tra le principali misure figurano la minimizzazione dei dati, la pseudonimizzazione e, ove opportuno, la cifratura, la separazione tra dati identificativi e dati di ricerca, il controllo degli accessi mediante autenticazione forte e profilazione degli utenti, la tracciabilità delle operazioni (logging), il monitoraggio degli eventi di sicurezza, la gestione delle vulnerabilità, l'aggiornamento dei sistemi, le procedure di backup e disaster recovery, nonché specifiche procedure per la gestione degli incidenti di sicurezza e delle violazioni dei dati personali (data breach).

Trattamenti aventi ad oggetto dati sottoposti a maggiore tutela.

Per i trattamenti riguardanti dati genetici, dati relativi all'HIV, all'interruzione volontaria di gravidanza, alla vita sessuale e alle ulteriori categorie individuate dalla DPIA, il modello prevede misure di sicurezza rafforzate, in considerazione della maggiore incidenza sui diritti e sulle libertà degli interessati. Tali misure comprendono, tra l'altro, una più rigorosa limitazione degli accessi ai soli soggetti autorizzati, la segregazione logica dei dati, tecniche di pseudonimizzazione e cifratura rafforzate, specifiche modalità di gestione e conservazione dei dati e dei campioni biologici, procedure dedicate per la comunicazione degli esiti e degli incidental findings, nonché ulteriori garanzie organizzative e procedurali volte a ridurre il rischio di reidentificazione, utilizzi impropri o trattamenti non autorizzati.



Trattamenti effettuati mediante nuove tecnologie.

La DPIA dedica uno specifico approfondimento ai trattamenti che impiegano piattaforme digitali per la ricerca (quali REDCap), sistemi di intelligenza artificiale, algoritmi, strumenti di machine learning, dispositivi IoT e dati sintetici. Per tali trattamenti, alle ordinarie misure di sicurezza si affiancano specifiche misure di governance tecnologica, finalizzate a garantire la supervisione umana dei processi, la trasparenza e la verificabilità dei sistemi algoritmici, la valutazione e il monitoraggio dei bias, la qualità e l'affidabilità dei dati utilizzati, il controllo continuo delle prestazioni dei sistemi, nonché il costante riesame dei rischi connessi all'evoluzione tecnologica.

Sulla base delle misure previste e delle valutazioni effettuate, il rischio residuo viene considerato generalmente **basso o accettabile**, senza evidenza di rischi tali da richiedere consultazione preventiva dell'Autorità Garante, fermo restando l'obbligo di aggiornamento periodico della DPIA, previsto con cadenza triennale o al verificarsi di modifiche normative, organizzative o tecnologiche rilevanti.

In conclusione, la DPIA Madre costituisce uno strumento metodologico uniforme per la gestione dei trattamenti di dati personali nell'ambito della ricerca sanitaria, fornendo alle Aziende sanitarie un modello condiviso per l'identificazione dei rischi, la selezione delle misure di sicurezza e la documentazione delle valutazioni richieste dall'art. 35 del GDPR. Il modello favorisce un approccio omogeneo all'interno delle Aziende dell'Area Vasta Emilia Centro, assicurando elevati standard di protezione dei dati personali, promuovendo la conformità normativa e supportando lo sviluppo della ricerca scientifica mediante un sistema di garanzie tecniche, organizzative e procedurali improntato ai principi di responsabilizzazione, proporzionalità, minimizzazione del rischio e miglioramento continuo.