SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Modena

Il Direttore Generale

Visti:

- l'art. 35 del Regolamento (UE) 2016/679 – GDPR secondo il quale "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali";
- l'art. 110, co. 1 del Codice Privacy, da ultimo modificato con L. 56/2024, a norma del quale "Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario [...] quando a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice".
- il Provvedimento del Garante per la protezione dei dati personali N. 514/2018 recante "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101", come modificato dal Provvedimento della medesima Autorità n. 298 del 9 maggio 2024 volto ad "individuare le garanzie di cui all'art. 110 del Codice e [...] a promuovere l'adozione di nuove Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, ai sensi degli artt. 2-quater e 106 del Codice";
- il Provvedimento del Garante per la protezione dei dati personali N. 146/2019, "recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101", in particolare gli allegati 4 "Prescrizioni relative al trattamento dei dati genetici" e 5 "Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica";

Ritenuto, alla luce ed in applicazione della sopra richiamata normativa, di provvedere alla predisposizione di uno schema di Valutazione di Impatto sulla protezione dei dati personali (DPIA) relativamente al trattamento dei dati personali effettuato dall'Azienda Ospedaliero-Universitaria di Modena ai fini di ricerca scientifica in campo medico, biomedico o epidemiologico, con riferimento a tutti gli studi, anche multicentrici, condotti dalla Azienda stessa in qualità di promotore, nello specifico per i casi in cui, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca;

Dato atto inoltre che in generale il trattamento dei dati personali per finalità di ricerca rientra nei casi, dettati dall'art. 35, par. 3 del GDPR, per i quali è prevista la necessaria conduzione di una DPIA, ovvero:

- trattamenti sistematici ed estensivi di valutazione di aspetti personali dell'interessato, basati su sistemi automatizzati, inclusa la profilazione, i cui esiti portino a decisioni che possono avere effetti legali diretti ed indiretti sull'interessato (ex articolo 35, paragrafo 3, lett. a) del GDPR);
- trattamenti, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, (ex articolo 35, comma 3, lett. b) del GDPR);
- altre attività di trattamento che siano inserite nell'elenco pubblico dell'Autorità Garante nazionale e che richiedono specificamente lo sviluppo di una DPIA (cfr. Allegato n. 1 al Provvedimento Garante Privacy n. 467 dell'11/10/2018);

e che a tali casistiche generali si aggiungono i trattamenti per i quali la valutazione d'impatto è prevista da disposizioni normative e/o regolamenti, come nel predetto art. 110 del Codice Privacy.
Acquisito per le vie brevi, oltre che in calce a questo documento, il parere favorevole del DPO in merito all' esito del modulo DPIA Versione 1.0 del 03.02.2025, ai sensi degli artt. 35, par. 2 e 39 GDPR;

- approva la Valutazione di Impatto sulla protezione dei dati relativamente al trattamento dei dati personali (DPIA) effettuato dall'Azienda Ospedaliero-Universitaria di Modena ai fini di ricerca scientifica in campo medico, biomedico o epidemiologico, con riferimento a tutti gli studi, anche multicentrici, condotti dalla Azienda stessa in qualità di promotore, quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca;

- dispone, con riferimento agli studi che rispettano i requisiti indicati nella presente DPIA, di non procedere alla consultazione della Autorità Garante per la protezione dei dati personali, non rilevando la predetta DPIA un rischio elevato per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

Parere favorevole DPO
Azienda Ospedaliero-Universitaria di Modena
Erica Molinari
(firmato digitalmente)

Erica
Molinari
08.03.2025
09:31:15
GMT+01:00

Per il Titolare
Il Direttore Generale
Azienda Ospedaliero-Universitaria di Modena
Luca Baldino
(firmato digitalmente)

LUCA
BALDINO
13.03.2025
16:00:21
GMT+01:00

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI - DPIA

Trattamento in esame: trattamento di dati personali per fini di ricerca scientifica in campo medico, biomedico o epidemiologico

ai sensi dell'art. 110, comma 1, secondo periodo del D.Lgs 196/2003 e s.m.i.

Descrizione del trattamento	Attività di ricerca scientifica in campo medico, biomedico o epidemiologico ai sensi dell'art. 110, comma 1, secondo periodo, del D.Lgs. 196/2003, nonché attività amministrative connesse.
Titolare del trattamento	Azienda Ospedaliero-Universitaria di Modena
Team elaborazione DPIA	Ufficio Privacy, Ufficio Ricerca, Servizio Tecnologie dell'Informazione
RPD/DPO	Erica Molinari
Data di avvio	2025
Data validazione DPO	2025
Frequenza di aggiornamento prevista	Annuale

INDICE

1 CONTESTO GENERALE

Presso l'Azienda Ospedaliero-Universitaria di Modena, l'attività di ricerca è svolta in piena coerenza con le disposizioni dell'ordinamento in materia di protezione dei dati.

Nella norma, prima dell'avvio di ogni progetto di ricerca, viene sottoposto all'autorizzazione del Comitato Etico competente un protocollo corredato di un dettagliato documento informativo per l'acquisizione del consenso informato.

Inoltre è prevista la consegna ai pazienti arruolati di una Informativa sul trattamento dei dati personali dedicata, redatta ai sensi dell'art. 13 del GDPR (o dell'art. 14 qualora i dati siano stati raccolti presso altro titolare). Analogamente è prevista l'acquisizione di uno specifico consenso al trattamento dei dati personali, ove necessario e possibile ai sensi dell'art. 110 del Codice Privacy.

Coerentemente con l'allegato 5 del Provvedimento dell'Autorità Garante n. 146 del 5 giugno 2019 recante le "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101" per ogni ricerca è prevista la redazione di un protocollo, nel quale si dà conto della tipologia dei dati trattati e delle operazioni più significative da realizzare col trattamento in questione, nonché della sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

Inoltre, nel caso in cui il protocollo preveda la comunicazione dei dati personali tra i centri partecipanti/collaboranti sono stipulati specifici accordi per la protezione dei dati.

Infine, a norma dell'art. 7 della Legge Regionale 01 giugno 2017, n. 9, recante la "Fusione dell'Azienda Unità Sanitaria Locale di Reggio Emilia e dell'Azienda Ospedaliera 'Arcispedale Santa Maria Nuova'. Altre disposizioni di adeguamento degli assetti organizzativi in materia sanitaria", l'attività di ricerca e sperimentazione clinica è consentita esclusivamente alla luce del rilascio del nulla osta da parte del Rappresentante Legale dell'Azienda/Titolare del trattamento dei dati o di suo delegato.

Con riferimento all'attività di valutazione di impatto del trattamento di dati personali per finalità di ricerca, nel mese di giugno 2024, approfittando della esigenza di confronto sulle intervenute modifiche normative in materia (L. 56/2014 di modifica dell'art. 110 Codice Privacy; nuove Garanzie introdotte dal Garante Privacy per la corretta applicazione dell'art. 110 del Codice Privacy, di cui al Provvedimento del 298/2024) le Aziende Sanitarie di Modena (AUSL e AOU) e di Reggio Emilia hanno avviato una riflessione in merito alle modalità di svolgimento di dette valutazioni, allo scopo di semplificarne la conduzione/compilazione, pur nel rispetto dei principi e delle norme di settore e di ricondurre tutta l'attività di ricerca, in particolare laddove condotta in assenza di informativa e consenso degli interessati, ad un unico schema-tipo di valutazione di impatto.

Alla luce di quanto sopra esposto, è stata predisposto uno schema-tipo di DPIA che ogni Azienda utilizzerà per l'adozione della propria valutazione d'impatto nelle attività di ricerca. Presso ogni Azienda saranno di conseguenza eventualmente revisionati i percorsi tesi alla regolamentazione delle attività di ricerca e di sperimentazione.

Viene pertanto adottata la presente DPIA avente ad oggetto l'attività di ricerca condotta in assenza di informativa e consenso degli interessati sussistendo le ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

La presente Valutazione d'impatto è soggetta ad aggiornamento e revisione annuale ed è pubblicata sul sito web istituzionale delle Aziende interessate.

Finalità del documento

Il trattamento di dati personali deve avvenire nel rispetto della normativa applicabile in materia di protezione dei dati personali e, in particolare, delle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito, il "Regolamento" o "GDPR") e del D. Lgs. n. 196 del 30 giugno 2003 (Codice in materia di protezione dei dati personali – di seguito, il "Codice Privacy").

I dati, inoltre, devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità e, comunque, "adeguati, pertinenti e limitati a quanto necessario alle finalità per le quali sono trattati" (principi della limitazione della finalità e di minimizzazione dei dati - art. 5, par. 1, lett. b) e c) del Regolamento).

Si evidenzia inoltre che i dati personali devono essere "trattati in modo lecito corretto e trasparente" (principio di "liceità, correttezza e trasparenza" e "in maniera da garantire un'adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti (principio di "integrità e riservatezza")" (art. 5, par. 1, lett. a) e f) del Regolamento).

Il Regolamento prevede poi che il titolare del trattamento valuti i rischi che un trattamento può determinare sui diritti e libertà fondamentali degli interessati e, conseguentemente, metta in atto "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio", tenendo conto, tra l'altro "della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (art. 32 del Regolamento).

Pertanto, lo scopo del presente documento è quello di fornire una valutazione dell'impatto che il trattamento dei dati, relativo all'attività di ricerca, potrebbe avere sui diritti e sulle libertà dei soggetti interessati, al fine di valutare l'entità del rischio, rapportata alla necessità e alla proporzionalità del trattamento stesso.

Tale valutazione è necessaria, dunque, per consentire la gestione dei rischi derivanti dal trattamento stesso, anche attraverso la programmazione di misure organizzative e tecniche idonee a garantire il rispetto delle disposizioni in materia di trattamento dei dati personali.

Ambito oggettivo di applicazione

La presente valutazione ha ad oggetto il trattamento[1] dei dati personali nell'attività di ricerca condotta sull'essere umano, in ogni sua modalità di realizzazione, in particolare per tutti i progetti di ricerca condotti in assenza di informativa e consenso degli interessati, sussistendo le ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

In generale, il trattamento dei dati per finalità di ricerca rientra nei casi, dettati dall'art. 35, par. 3 del GDPR, per i quali è prevista la necessaria conduzione di una DPIA, ovvero:

- trattamenti sistematici ed estensivi di valutazione di aspetti personali dell'interessato, basati su sistemi automatizzati, inclusa la profilazione, i cui esiti portino a decisioni che possono avere effetti legali diretti ed indiretti sull'interessato (ex articolo 35, paragrafo 3, lett. a) del GDPR);
- trattamenti, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, (ex articolo 35, comma 3, lett. b) del GDPR);
- altre attività di trattamento che siano inserite nell'elenco pubblico dell'Autorità Garante nazionale e che richiedono specificamente lo sviluppo di una DPIA (cfr. Allegato n. 1 al Provvedimento Garante Privacy n. 467 dell'11/10/2018);

A tali casistiche generali si aggiungono i trattamenti per i quali la valutazione d'impatto è prevista da disposizioni normative e/o regolamenti, come nel predetto art. 110 del Codice Privacy.

Categorie di dati personali trattati

L'attività di ricerca prevede il trattamento dei dati personali di soggetti interessati arruolati negli studi condotti presso Azienda Ospedaliero-Universitaria di Modena /Titolare del trattamento. Tra questi soggetti rientrano anche pazienti sottoposti a prestazioni sanitarie nell'ambito della normale pratica clinica; i pazienti possono essere anche minori e persone temporaneamente incoscienti (ad es. in coma, e interdetti/inabilitati).

I dati personali comprendono:

- dati anagrafici (ad es. sesso).
- dati antropometrici, dati relativi alla salute raccolti durante le visite, i ricoveri, gli accessi al pronto soccorso, nonché gli esami e gli accertamenti effettuati presso l'Azienda. In particolare, i dati riguardano diagnosi, interventi, terapie somministrate, esiti degli esami di laboratorio, di dispositivi, campioni biologici, dati genetici (secondo la definizione fornita dal Garante nell'allegato 4 al Provvedimento n. 146/2019), immagini.

Il trattamento di dati per finalità di ricerca in esame, considerato l'utilizzo di strumenti informatizzati, potrebbe riguardare anche il trattamento dei dati personali dei *caregiver* e dei rappresentanti dei soggetti in ricerca, degli operatori convolti nel progetto di ricerca, tra i quali dati anagrafici, dati di contatto (indirizzo e-mail) e i log delle attività svolte.

[1] Ai sensi dell'art. 4, n. 2) per "trattamento" si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"

L’attività di trattamento oggetto della presente DPIA, dunque, considerate le categorie dei dati personali da trattare potrebbe presentare un rischio elevato per i diritti e le libertà delle persone fisiche, secondo i criteri di cui all’art. 35, paragrafo 3, del GDPR.

Modalità di raccolta dei dati personali

Nell’ambito dell’attività di ricerca, di norma i dati sono forniti direttamente dal soggetto interessato (o da soggetti che esercitano nei confronti dell’interessato la responsabilità genitoriale, o rivestono la qualifica di tutori o amministratori di sostegno) o da soggetti terzi (medico specialista di riferimento, medico di base, ASL, Comune, Autorità diverse, etc.), previa verifica della legittimità del trattamento e della finalità di raccolta, anche in coerenza con quanto è definito nel protocollo di ricerca sottoposto all’approvazione del Comitato Etico competente.

Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l’informativa e l’acquisizione del consenso, salve le deroghe normative, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia.

I dati possono essere acquisiti d’ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente (ad es. studi epidemiologici; Registro tumori).

La raccolta dei dati, intesa come inserimento nella scheda raccolta dati (di seguito anche eCRF), non avviene di norma con riferimento ai dati personali in chiaro dell’interessato, ma esclusivamente mediante ID univoco associato all’anagrafica che identificherà i dati dell’interessato all’interno dei registri di studio. L’associazione ID/anagrafica è gestita e archiviata su un file differente da quello utilizzato per la raccolta, e la eventuale successiva trasmissione dei dati al Promotore/CRO e avviene sotto la responsabilità del PI a cui sono assegnate credenziali personali non trasferibili per accedere e validare le informazioni inserite nel eCRF.

Base giuridica del trattamento dei dati per finalità di ricerca

Il GDPR introduce una specifica deroga al divieto di trattamento delle particolari categorie di dati per scopi di ricerca, ammettendo che essi possano essere trattati per tali scopi sulla base del diritto dell'Unione Europea e nazionale. Tale trattamento deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, in conformità dell'articolo 89, paragrafo 1 del GDPR stesso (art. 9, par. 2, lett. j) del Regolamento).

Nel solco dello spazio normativo lasciato al legislatore nazionale da tale ultima disposizione, il legislatore italiano ha confermato la necessità di acquisire il consenso quale base giuridica del trattamento di dati personali per finalità di ricerca e ha inoltre mantenuto, modificandola – e integrando il GDPR a livello nazionale - la medesima disposizione previgente del Codice Privacy in tema di Ricerca medica, biomedica ed epidemiologica, ovvero l’art. 110, prevedendo fattispecie di eccezione alla acquisizione del consenso, purché accompagnate da specifiche misure di garanzia.

Il comma 1 dell’art. 110, da ultimo modificato dalla L. 56/2024, dispone infatti che “Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di Ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la Ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la Ricerca rientra in un programma di Ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento

delle finalità della Ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di Ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice".

Pertanto, nell'ordinamento italiano, le basi giuridiche del trattamento per finalità di ricerca e sperimentazione clinica sono costituite, da:

- art. 9, par. 2 lettera a) del GDPR - consenso
- art. 110, comma 1, primo periodo del Codice Privacy - ricerca effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione Europea in conformità all'articolo 9, paragrafo 2, lettera j), del GDPR
- art. 110, comma 1, secondo periodo del Codice Privacy - impossibilità di acquisire il consenso degli interessati (coerentemente con l'Allegato 5 del Provvedimento dell'Autorità Garante n. 146/2019 recante le "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101"),
- art. 110-bis, comma 4 del Codice Privacy – applicabile solamente agli IRCCS.

Per quanto riguarda le "ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta impossibile o implica uno sforzo sproporzionato oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della Ricerca", l'Allegato 5 del "Provvedimento dell'Autorità Garante n. 146/2019 recante le "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101" prevede che esse si rinvengano in:

1. motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione. Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione della ricerca la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento);
2. motivi di impossibilità organizzativa riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per la ricerca in termini di alterazione dei relativi risultati; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dalla ricerca, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti (ad esempio, nei casi in cui la Ricerca riguarda interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute). Con riferimento a tali motivi di impossibilità organizzativa, le prescrizioni dell'Autorità concernono anche il trattamento dei dati di coloro i quali, all'esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente) risultino essere al momento dell'arruolamento nella ricerca:
   - deceduti o
   - non contattabili.

   Resta fermo l'obbligo di rendere l'informativa agli interessati inclusi nella ricerca in tutti i casi in cui, nel corso della ricerca, ciò sia possibile e, in particolare, laddove questi si rivolgano al centro di cura,

anche per visite di controllo, anche al fine di consentire loro di esercitare i diritti previsti dal Regolamento;

3. motivi di salute riconducibili alla gravità dello stato clinico in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso. In tali casi, la ricerca deve essere volta al miglioramento dello stesso stato clinico in cui versa l'interessato. Inoltre, occorre comprovare che le finalità della Ricerca non possano essere conseguite mediante il trattamento di dati riferiti a persone in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso o con altre metodologie di ricerca. Ciò, avuto riguardo, in particolare, ai criteri di inclusione previsti dalla ricerca, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché all'attendibilità dei risultati conseguibili in relazione alle specifiche finalità della ricerca. Con riferimento a tali motivi, deve essere acquisito il consenso delle persone indicate nell´art. 82, comma 2, lett. a), del Codice come modificato dal d.lgs. n. 101/2018. Ciò, fermo restando che sia resa all'interessato l'informativa sul trattamento dei dati non appena le condizioni di salute glielo consentano, anche al fine di consentirgli l'esercizio dei diritti previsti dal Regolamento.

In coerenza con le più recenti pronunce dell'Autorità Garante, l'impossibilità di acquisire il consenso è accertata in occorrenza di tre tentativi infruttuosi di raccolta, i quali devono registrati nella cartella clinica dei pazienti interessati[2].

Infine, tra gli altri, si richiamano i seguenti riferimenti:

1. Dichiarazione di Helsinki (WMA Declaration Of Helsinki – Ethical Principles For Medical Research Involving Human Subjects).

2. Convenzione di Oviedo "per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazione della biologia e della medicina: Convenzione sui Diritti dell'Uomo e la biomedicina" del 4 aprile 1997.

3. DM 15 luglio 1997 "Recepimento delle line guida dell'Unione Europea di buona pratica clinica per la esecuzione delle sperimentazioni cliniche dei medicinali" e s.m.i.

4. Clinical Trials Regulation (Regulation (EU) No 536/2014).

5. Regole Deontologiche per trattamenti a fini statistici o di Ricerca scientifica (Provvedimento dell'Autorità Garante del 19 dicembre 2018 n. 515), modificato con Provvedimento n. 298 del 9 maggio 2024, al fine di individuare le garanzie di cui all'art. 110, comma 1, del Codice Privacy, a seguito della modifica intervenuta con la L. 56/2024.

6. Provvedimento dell'Autorità Garante n. 146 del 5 giugno 2019 recante le "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101"

Informativa e Consenso

Il trattamento dei dati personali effettuato nell'ambito della ricerca, nelle sue diverse forme, è descritto in forma chiara ed intellegibile, nell'informativa ex artt. 13 e 14 del GDPR, in cui sono elencate finalità e modalità del trattamento quale condizione principale del dovere del titolare di assicurare la trasparenza e la correttezza dei trattamenti effettuati.
L'informativa resa ai sensi dell'art. 13 del GDPR (o dell'art. 14 GDPR nel caso in cui i dati non siano stati ottenuti presso l'interessato) viene fornita all'interessato (ivi compresi genitori/tutori/amministratori di

[2] Garante doc web 9960973 del 26.10.2023 e doc web 9988614 del 24.01.2024

sostegno) arruolabile nella ricerca, di norma durante l'incontro di presentazione della ricerca o, nel caso degli studi retrospettivi, durante un contatto successivo alla raccolta del dato.
In tale occasione, ove necessario e possibile, viene anche raccolto il consenso specifico al trattamento dei dati.
Nell'informativa sono, altresì, comunicati agli interessati la durata della ricerca, i tempi e le modalità di trattamento e di conservazione dei dati.

Pubblicazione e Trasparenza

Ai sensi dell'art. 110, comma 1, secondo periodo del Codice Privacy e nel rispetto delle garanzie individuate dal Provvedimento dell'Autorità Garante n. 298 del 9 maggio 2024, nel caso di studi che prevedano trattamenti di dati sulla salute per finalità di ricerca medica, biomedica e epidemiologica, riferiti a soggetti deceduti o non contattabili per motivi etici o organizzativi, la Valutazione d'impatto è oggetto di pubblicazione sul sito web istituzionale della Azienda, nella sezione dedicata all'attività di ricerca.

Unitamente alla DPIA sarà resa pubblica anche l'informativa per il trattamento dei dati personali, resa ai sensi dell'art. 13 del GDPR (o dell'art. 14 GDPR nel caso in cui i dati non siano stati ottenuti presso l'interessato).

2 CRITERI E METODOLOGIA

Valutazione preliminare dell'utilizzo dei dati

Come verranno raccolti i dati?

L'attività di ricerca e di sperimentazione clinica, analizzata dal presente documento, prende in esame i dati personali, compresi i dati di natura particolare, raccolti attraverso varie fonti a seconda della tipologia della ricerca da realizzare. Di seguito si elencano sinteticamente, a titolo di esempio, alcune fonti di raccolta dei dati:

a) interessati;
b) cartelle cliniche ed ambulatoriali;
c) database e applicativi;
d) open data;
e) dataset prodotti da soggetti pubblici o privati, nazionali o internazionali;
f) database interni ed esterni;
g) biobanche;
h) applicativi informatici;
i) dispositivi elettronici;
j) IOT (Internet of Things);
k) data lake.

Chi avrà accesso ai dati?

Per le attività di ricerca e di sperimentazione clinica: PI e team di ricerca identificati in base al Delegation Log dello studio e autorizzati dalla Direzione Aziendale.

Per le attività di manutenzione dei sistemi informativi: servizio IT, SUIC ed eventuali fornitori (nominati responsabili del trattamento ai sensi dell'art. 28 GDPR).

Per le attività di vigilanza: Funzione Privacy Aziendale e il DPO.

Per le attività di monitoraggio e audit: Servizio Formazione, Ricerca e Innovazione

Per le attività di rimborso delle spese sostenute dai soggetti arruolati nella Ricerca: l'Ufficio competente individuato dall'Azienda/Istituto.

Tutti i soggetti sopra elencati sono delegati o autorizzati al trattamento dei dati per lo svolgimento delle proprie funzioni istituzionali, nel rispetto della policy aziendale.

In che modo i dati verranno eventualmente condivisi?

Qualora la raccolta dei dati non avvenga mediante apposito software, il trasferimento ad eventuali soggetti esterni (ad esempio Centro Partecipante/Centro Collaboratore/CRO) di documenti contenenti dati raccolti all'interno degli studi può avvenire attraverso:

- la PEC;
- la posta elettronica ordinaria, in tal caso allegando i documenti in formato criptato e inviando la chiave di decriptazione con altro strumento di comunicazione;
- altri strumenti di comunicazione sicura eventualmente implementati nel tempo dalla Azienda: attraverso i processi di autenticazione e autorizzazione, i destinatari dei dati potranno accedere alle piattaforme condivise per l'estrazione del dataset. L'abilitazione all'accesso dei dati dopo la cessazione della ricerca è definita in funzione del ruolo svolto nella ricerca dall'amministratore di sistema. Per i centri esterni la validità delle utenze sarà comunque limitata al periodo della sperimentazione.

La comunicazione e il trasferimento dei dati per i trattamenti connessi alla presente valutazione d'impatto può avvenire previa sottoscrizione di un accordo specifico e comunque, in coerenza con quanto previsto dalla normativa vigente e pattuito nel protocollo di ricerca.

Come verranno archiviati, aggiornati ed eliminati i dati quando non più necessari?

I dati relativi agli studi saranno aggiornati in funzione delle attività svolte nelle varie fasi previste della ricerca stessa, archiviati per il tempo definito in ogni protocollo di ricerca ed eliminati al termine temporale anch'esso definito nel protocollo di ricerca e nell'informativa per il trattamento dati personali.

I dati contenuti nelle fonti, di cui sopra, seguono il ciclo di vita proprio definito dalla normativa di settore (massimario di scarto).

Valutazione del rischio

Di seguito sono elencati i criteri volti a valutare il rischio e la conseguente applicabilità della presente DPIA.

Tecnologie utilizzate

In questo trattamento verranno utilizzate nuove tecnologie informatiche che potrebbero avere un significativo potenziale di violazione della protezione dei dati personali e riduzione del livello di protezione dei dati, che bisogna garantire agli interessati?

No.
I dati raccolti su eCRF o su foglio di lavoro elettronico, in ossequio al principio di minimizzazione, sono esclusivamente quelli definiti nel protocollo della ricerca e sono resi in forma pseudonimizzata.

Nel caso di utilizzo di piattaforme installate su server aziendale (es. RedCAP) o in altre piattaforme messe a disposizione dai partner di progetto, occorre fare riferimento alla specifica DPIA aziendale o alla DPIA predisposta da questi ultimi.

Metodi di identificazione degli interessati

In ossequio alle procedure e ai regolamenti aziendali, il riconoscimento dei soggetti reclutati avviene attraverso sistemi tradizionali, quali ad esempio la carta di identità o altro documento di riconoscimento. Negli studi retrospettivi l'identificazione può essere effettuata anche attraverso codificazioni derivanti da numeri nosologici o codici di pseudonimizzazione assegnati in fase di rilevazione e registrati in appositi database.

Allo stato attuale non sono previsti ulteriori metodi di identificazione intrusivi e/o onerosi per l'interessato (es. dati biometrici).

Coinvolgimento di altre strutture

Questa iniziativa di trattamento coinvolge altre strutture, sia pubbliche, sia private, sia appartenenti a settori non-profit e volontari?

Nelle ricerche che coinvolgono più di un centro partecipante/collaborante (ad es. negli studi multicentrici) il coinvolgimento di altri soggetti pubblici o privati può essere regolato da atti giuridici che definiscono compiti e responsabilità.

L'attività di ricerca di tipo multicentrico prevede la partecipazione di soggetti pubblici o privati (anche appartenenti a enti no profit e di volontariato) nelle modalità previste dal protocollo di ricerca.

Modifiche alle modalità di trattamento dei dati

Il trattamento apporterà nuove o significative modifiche alle modalità di trattamento dei dati personali, che potrebbero destare preoccupazioni dell'interessato?

L'informativa resa agli interessati contiene tutti gli elementi necessari a far sì che il trattamento sia compreso in tutte le sue fasi e modalità di esecuzione; pertanto, non si ritiene che si possano verificare situazioni di preoccupazione o incertezze derivanti dal trattamento.

I dati personali, propri di un interessato, già presenti in un esistente database, verranno assoggettati a nuove o modificate modalità di trattamento?

No, poiché nei casi in cui la ricerca sia retrospettiva la fonte dei dati è costituita dai documenti clinici già formati per finalità di cura, quindi non modificabili.

Questa iniziativa di trattamento apporterà nuove o significative modifiche alle modalità di consolidamento, interscambio, riferimenti incrociati, abbinamento di dati personali, provenienti da più sistemi di trattamento?

Gli studi che prevedono l'utilizzo di nuove tecnologie potrebbero modificare le modalità di trattamento in uso, ma tali evenienze verranno effettuate a seguito dell'adozione di misure di sicurezza adeguate, così come previsto dall'art. 32 del GDPR e descritto nell'informativa ex art. 13 e 14 GDPR.

Modifiche alle procedure di trattamento dei dati

Questo trattamento potrà introdurre nuove modalità e procedure di raccolta dei dati, che non siano sufficientemente trasparenti?

L'informativa resa agli interessati contiene tutti gli elementi che descrivono le modalità di raccolta; pertanto, si ritiene che le procedure siano trasparenti e che non si possano verificare situazioni di intrusività nella sfera personale non conosciuta o non condivisa.

Questo trattamento introdurrà nuove o modificate modalità di conservazione dei dati non chiare o prolungate oltremodo?

No, le modalità di conservazione non verranno innovate o modificate.

I riferimenti riguardo ai tempi di conservazione sono espressamente indicati e resi noti attraverso l'informativa e fanno riferimento al protocollo di ricerca o sono determinati dal massimario di scarto.

Questo trattamento modificherà le modalità di messa a disposizione dei dati?

No, il trattamento non prevede una modifica alle modalità con le quali i dati sono messi a disposizione.

Esenzioni dalla applicazione delle disposizioni del GDPR (ex art.2, paragrafo 2 GDPR)

L'attività di trattamento esula dall'ambito delle disposizioni legislative dell'Unione Europea?

Per i Paesi al di fuori dello Spazio Economico Europeo (extra UE) i dati saranno trasferiti esclusivamente nel caso in cui sia stata emanata una decisione di adeguatezza o nei seguenti casi:

- se l'interessato è stato informato dal titolare dell'assenza di una decisione di adeguatezza e dei conseguenti rischi e ha espresso il proprio consenso al trasferimento;
- sulla base di accordi/contrattuali stipulati che forniscono garanzie adeguate agli interessati (Clausole Contrattuali Standard);
- per i gruppi di imprese, (così come disciplinati dal GDPR e secondo la classificazione del Codice Civile, ad es. imprese collegate/partecipate) sulla base di norme vincolanti di impresa che devono essere approvate dall'autorità competente (in Italia, l'Autorità Garante della Privacy);
- qualora il trasferimento sia necessario per l'esecuzione di un contratto concluso su richiesta dell'interessato e il titolare;
- sulla base dell'adesione al Data Privacy Framework (DPF), che consente una tutela adeguata degli interessati nei trasferimenti di dati personali tra Europa e Stati Uniti d'America.

Trasparenza e pubblicità

Le finalità del trattamento sono chiare e sufficientemente pubblicizzate?

Il trattamento dei dati personali, effettuato nell'ambito della ricerca, nelle sue diverse forme è descritto in forma chiara ed intellegibile, nell'informativa ex artt. 13 e 14 del GDPR.
Nel suddetto documento sono elencate finalità e modalità del trattamento quale condizione principale del dovere del titolare di assicurare la trasparenza e la correttezza dei trattamenti effettuati.
Sul sito Istituzionale saranno pubblicati i documenti inerenti alle attività di ricerca (informativa, DPIA, ecc.).

Decisione su come procedere

Tenendo conto della tipologia di trattamento e in conformità delle indicazioni previste all'articolo 35, paragrafo 3 del GDPR, è necessario effettuare la DPIA sul trattamento della Ricerca in ogni sua declinazione.

Congruità con altre leggi, codici o regolamenti afferenti alla protezione dei dati

In relazione al provvedimento dell'Autorità Garante n. 146/2019, è stata effettuata una verifica di conformità al medesimo secondo quanto illustrato nell'Appendice A e si è giunti alla conclusione che l'attività di trattamento oggetto della presente DPIA è conforme alle prescrizioni del provvedimento indicato.

Contenuti analitici della DPIA

Descrizione analitica delle operazioni di trattamento, con indicazione delle finalità perseguite dal titolare del trattamento

I dati personali degli interessati e quelli appartenenti a particolari categorie (compresi i dati a maggior tutela quali quelli dei soggetti minori, donne vittime di violenza, ecc..) sono raccolti e trattati per finalità di ricerca le cui caratteristiche e modalità sono descritte nel dettaglio nell'informativa ex art. 13 GDPR e nel protocollo della ricerca.

Valutazione della necessità e proporzionalità delle operazioni di trattamento, in relazione alle finalità

La necessità e la proporzionalità delle operazioni di trattamento si valutano in maniera positiva in quanto sono presenti le seguenti misure:

- finalità determinate, esplicite e legittime;
- liceità del trattamento;
- dati personali adeguati, pertinenti e limitati a quanto necessario;
- limitazione della conservazione.

Valutazione dei rischi che incidono sui diritti e le libertà degli interessati, incluso il rischio di discriminazione connesso o rinforzato dal trattamento

L'analisi condotta nelle sezioni precedenti, tenendo conto delle misure tecniche ed organizzative nonché degli atti giuridici che talora sottendono il trattamento e che ne disciplinano le forme e le responsabilità degli attori (ad es. accordo di contitolarità, designazione responsabile di trattamento, accordi studi specifici), non ha rilevato rischi che possano incidere sui diritti e le libertà degli interessati, inclusi i rischi legati al rispetto dei principi di conoscibilità, non esclusività o di discriminazione algoritmica connessi o rinforzati dal trattamento attraverso l'utilizzo ad esempio delle tecniche di Intelligenza Artificiale.

Descrizione delle misure individuate per mettere sotto controllo i rischi e ridurre al minimo il volume di dati personali da trattare - Data Protection by Default

Al fine di ridurre il rischio per i diritti e le libertà fondamentali degli interessati è prevista la piena applicazione dei principi affermati dall'art. 5 GDPR. Nel dettaglio, i principi di:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Nell'Appendice C (allegata) vengono elencate le misure tecniche e organizzative adottate per mitigare i rischi per i diritti e le libertà degli Interessati

Illustrazione di quali procedure di data protection by design e data protection by default verranno adottate, in conformità all'articolo 32 GDPR

Gli interessati vengono informati nello specifico delle finalità e delle modalità di raccolta dati e verrà acquisito e conservato, ove previsto e possibile, il loro esplicito consenso al trattamento.

Verranno raccolte solo le informazioni necessarie ai fini della Ricerca e di norma vengono seguite le procedure per pseudonimizzare i dati. I dati raccolti all'interno della Ricerca sono registrati su CRF e/o eCRF e gestiti in database della Ricerca (ad esempio foglio di lavoro elettronico o piattaforme ad hoc come REDCap) con accesso limitato al PI e ai suoi delegati tramite credenziali personali.

Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati - art 35 GDPR

Il riesame di congruità del presente documento sarà effettuato di norma con cadenza annuale; tale periodo può variare in rapporto alle eventuali criticità rilevate durante le fasi del trattamento o a seguito di interventi normativi, regolatori, audit, eventuali modifiche organizzative che possono determinarsi nel corso della ricerca.

In tal caso, la revisione della DPIA verrà effettuata tempestivamente.

3 CONCLUSIONE

Il percorso si è concluso con la redazione di un documento articolato e completo che, come previsto dall'art. 35 del GDPR, è stato sottoposto a valutazione del DPO che ha rilasciato parere favorevole.

APPENDICE A – Sintesi della congruità del trattamento previsto con le esigenze di protezione dei dati

Domanda	Risposta
1. Quali categorie di dati personali vengono trattate?	Dati personali (età, sesso ecc.), dati clinici (diagnosi, trattamenti sanitari, trattamenti farmacologici, esiti di esami di laboratorio, esiti di visite cliniche specialistiche, dati genetici, immagini ecc.)
2. Se vengono trattati speciali categorie di dati, elencati all'articolo 9 comma 1 GDPR, sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento?	Sì, quale parte fondamentale del processo di conduzione dell'attività di ricerca.
3. Vi sono aspetti afferenti al rispetto dell'articolo 2, comma 2, del GDPR, che protegge i diritti fondamentali e le libertà delle persone fisiche, ed in particolare il loro diritto alla protezione dei dati personali, che non siano trattati in questa DPIA?	NO
4. Tutti i dati personali che verranno trattati sono coperti da garanzie di riservatezza? Se sì, come viene garantita?	Sì, i dati vengono trattati solo da soggetti autorizzati inoltre i dati sono sempre pseudonimizzati o anonimizzati.
5. Come viene offerta agli interessati l'informativa in merito al fatto che i loro dati personali verranno raccolti e trattati?	L'informativa ai sensi dell'art. 13 o 14 GDPR viene fornita all'interessato, reclutato nella ricerca, di norma durante l'incontro di presentazione della ricerca o, nel caso degli studi retrospettivi, possibilmente durante un eventuale contatto successivo alla raccolta del dato. In tale occasione, viene anche raccolto il consenso specifico al trattamento dei dati. L'informativa viene inoltre pubblicata sul sito istituzionale dell'Azienda.
6. Il trattamento dei dati comporta l'utilizzo di dati personali già raccolti, che verranno utilizzati per finalità secondarie?	SI Inoltre, la possibilità del riuso deve essere descritta nell'informativa degli studi da cui provengono i dati e occorre aver acquisito, ove necessario e possibile, un nuovo consenso specifico.

7. Quali procedure vengono adottate per verificare che le modalità di raccolta dei dati sono adeguate, coerenti e non eccessive, in relazione alle finalità per i quali i dati vengono trattati?	Al fine di ridurre il rischio per i diritti e le libertà fondamentali degli interessati è prevista la piena applicazione dei principi affermati dall'art. 5 GDPR.
8. Con quali modalità viene verificata la accuratezza dei dati personali raccolti e trattati?	L'accuratezza dei dati personali raccolti viene garantita mediante gli identificatori utilizzati per l'estrazione: nome, cognome, data di nascita e codice fiscale dei pazienti inclusi nella ricerca.
9. È stata effettuata una valutazione circa il fatto che il trattamento dei dati personali raccolti potrebbe causare danni ai diritti e alle libertà agli interessati coinvolti?	Sì, tuttavia, non si ritiene che il trattamento effettuato, nelle varie fasi di ricerca, possa causare danni ai diritti e alle libertà degli interessati coinvolti in ragione delle misure di sicurezza adottate.
10. È stato stabilito un periodo massimo di conservazione dei dati?	Nel rispetto della normativa applicabile allo studio, i dati saranno conservati fino al termine indicato nel protocollo di ricerca, e indicati nel massimario di scarto salvo che gli interessati acconsentano alla conservazione per un periodo più lungo nell'ambito delle finalità del trattamento. I riferimenti riguardo ai tempi di conservazione sono espressamente indicati e resi noti attraverso l'informativa. Allo scadere del termine definito nel protocollo di ricerca i dati verranno distrutti o resi anonimi provvedendo alla cancellazione definitiva e irreversibile della corrispondenza tra il codice utilizzato sul dato e l'associazione di tale codice all'identità del partecipante.
11. Quali misure tecniche e organizzative di sicurezza sono state adottate per prevenire qualsivoglia trattamento di dati personali non autorizzato o illegittimo?	Accesso ai dati riservato – Solo personale avente diritto nell'ambito delle funzioni a cui è normalmente preposto accederà ai dati al fine di estrazione o immissione. Ognuna delle persone coinvolte nell'estrazione o immissione dei dati avrà accesso esclusivamente al sistema o ai documenti a cui è normalmente preposto. Pseudonimizzazione - il dataset in input, a seguito del processo di pseudonimizzazione restituirà in output il dataset pseudonimizzato, modificato rispetto al dato originale, e il dataset di transcodifica ad accesso riservato mediante password. Gestione postazioni: le postazioni utilizzate sono principalmente in dominio aziendale e le misure adottate sono quelle previste da regolamenti e

	policy aziendali. Controllo degli accessi fisici: l'accesso ai locali è consentito al solo personale che abbia necessità di accedere a dispositivi o attrezzature necessarie al trattamento, conservate in tali locali. Sicurezza dei documenti cartacei: in base alle istruzioni generali impartite dal Titolare, ogni singolo soggetto coinvolto nel trattamento dati per finalità di ricerca condivide la documentazione prodotta con i soli appartenenti al team di ricerca. Sicurezza dei canali informatici: tutte le postazioni e i dispositivi aziendali sono equipaggiati con strumenti di antispam, antivirus, sistemi di monitoraggio degli apparati fisici di rete e server e gestione degli alert. Gestione delle politiche di tutela della privacy: Il Titolare ha adottato Privacy Policy aziendali periodicamente revisionate, condivise con tutto il personale. Il personale viene adeguatamente formato in merito alle attività di trattamento e alle misure di sicurezza da adottare.
12. È previsto il trasferimento di dati personali in un Paese non facente parte dell'Unione europea? Se sì, quali provvedimenti sono stati adottati per garantire che i dati siano salvaguardati in modo appropriato?	Per i Paesi al di fuori dello Spazio Economico Europeo (extra UE) i dati saranno trasferiti esclusivamente nel caso in cui sia stata emanata una decisione di adeguatezza o nei seguenti casi: - se l'interessato è stato informato dal titolare dell'assenza di una decisione di adeguatezza e dei conseguenti rischi e ha espresso il proprio consenso al trasferimento; - sulla base di accordi/contratti stipulati che forniscono garanzie adeguate agli interessati (CCS - Clausole Contrattuali Standard); - per i gruppi di imprese, il trasferimento deve avvenire sulla base di norme vincolanti di impresa che devono essere approvate dall'autorità competente (in Italia, il Garante della Privacy); - il trasferimento è necessario per l'esecuzione di un contratto concluso su richiesta dell'interessato e il titolare;

	– sulla base dell'adesione al DPF (Data Privacy Framework che consente una tutela adeguata degli interessati nei trasferimenti di dati personali tra Europa e Stati Uniti d'America).

APPENDICE B - Tabella dei rischi afferenti alla DPIA

MATRICE DI VALUTAZIONE DEL RISCHIO

		IMPATTO§§				
PROBABILITA'	MOLTO ALTO§	5	10	15	20	25
	ALTO	4	8	12	16	20
	MEDIO	3	6	9	12	15
	BASSO	2	4	6	8	10
	MOLTO BASSO	1	2	3	4	5
		MOLTO BASSO	**BASSO**	**MEDIO**	**ALTO**	**MOLTO ALTO**

§ Frequenza con la quale si possono verificare criticità nel trattamento dei dati: **Rischio molto basso**: è probabile che non si verifichi mai; **Basso**: non è probabile che si verifichi, ma può accadere; **Medio**: si può verificare occasionalmente; **Alto**: è probabile che si verifichi, ma non in modo persistente/stabile; **Molto alto**: è quasi certo che si verifichi, possibilmente in modo frequente

§§ Impatto atteso: **Molto basso**: è improbabile che possa avere un qualsiasi impatto; **Basso**: può avere un impatto; **Medio**: è probabile che abbia un impatto; **Alto**: molto probabile che abbia un impatto significativo; **Molto alto**: correlato ad un impatto maggiore

Classificazione	Intervallo del rischio
Rischio Basso	Valore finale tra 1 e 6 compresi
Rischio Medio	Valore finale tra 7 e 11 compresi
Rischio Elevato	Valore finale tra 12 e 16 compresi

ACCESSO ILLEGITTIMO AI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Perdita di riservatezza dei dati personali coperti da segreto professionale; perdita del controllo dei propri dati; decifratura non autorizzata dei dati pseudonimizzati; diffusione dei dati non autorizzata; pregiudizio alla reputazione
Quali sono le principali minacce che potrebbero concretizzare il rischio?

Utilizzo inappropriato delle password di accesso ai pc aziendali e al database di raccolta dati; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; virus

Quali sono le fonti di rischio?

Fonti umane interne (lasciare incustodita la postazione di lavoro, errore di integrazione applicativa, sottrazione delle password di accesso da parte di un terzo). Fonti umane esterne (hacker, attacchi di ingegneria sociale). Fonti non umane (virus, applicativi che interoperano con il SW, introduzione di bug in seguito ad aggiornamento dell'applicativo)

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Istruzioni a persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Antivirus/firewall; Politiche di trasmissione dei dati;
Pseudonimizzazione

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Alta trattandosi di dati relativi alla salute

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Molto bassa: le politiche di sicurezza informatica e le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento

MINACCIA	VALORE DEL RISCHIO (P*I)	LIVELLO DI RISCHIO
ACCESSO ILLEGITTIMO	4*1	4 - BASSO

MODIFICHE INDESIDERATE DEI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

I dati dello studio non sono originali, pertanto la loro a modifica potrebbe avere conseguenze solo sulla attendibilità dei risultati dello studio e non sugli interessati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Utilizzo inappropriato delle password di accesso ai pc aziendali e al database di raccolta dati; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni e modificarle; attacco informatico; errata profilazione degli utenti; virus

Quali sono le fonti di rischio?

Fonti umane interne (lasciare incustodita la postazione di lavoro, alterazione volontaria di dati, errore umano involontario). Fonti umane esterne (hacker, attacchi di ingegneria sociale). Fonti non umane (virus, applicativi che interoperano con il SW)

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; antivirus/firewall; Back – up dei dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Molto bassa in quanto la modifica indesiderata non indice su dati originali e quindi sulla cura degli interessati

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Molto bassa: le politiche di sicurezza informatica e le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento

MINACCIA	VALORE DEL RISCHIO (P*I)	LIVELLO DI RISCHIO
MODIFICHE INDESIDERATE	1*1	1 - BASSO

PERDITA DI DATI

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Una perdita dei dati potrebbe causare l'alterazione dei risultati dello studio o la impossibilità di proseguirlo, tuttavia non si tratta di dati originali; pregiudizio alla reputazione; perdita di controllo sui propri dati personali

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Le principali minacce possono essere di natura informatica (infezione da ransomware che blocca il sistema di accesso ai propri database, provocando anche solo in modo temporaneo una impossibilità ad accedere al server, guasto che determina il danneggiamento, l'interruzione o la non disponibilità del sistema) o derivare da una azione umana (attacco hacker, attacchi di ingegneria sociale) o da Incidente tecnico al datacenter (incendio, inondazione, fulmini…)

Quali sono le fonti di rischio?

Fonti umane interne (operatori autorizzati che abusino del proprio ruolo o colposamente operino cancellazioni sui dati per inesperienza o imperizia; lasciare incustodita la postazione di lavoro; errore progettuale/realizzativo che opera una modifica impropria ai dati gestiti); Fonti umane esterne (hacker); Fonti di rischio non umane (virus informatico; calamità naturali; guasto all'impianto elettro-idraulico del datacenter)

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Back – up dei dati; Misure anti – intrusive; antivirus/firewall; Tracciabilità; Gestione postazioni; Politiche di tutela della privacy¸ Politiche di sicurezza informatica

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Alta trattandosi di dati relativi alla salute

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Molto bassa: le politiche di sicurezza informatica e le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento

MINACCIA	**VALORE DEL RISCHIO (P*I)**	**LIVELLO DI RISCHIO**
PERDITA DI DATI	4*1	4 - BASSO

VALUTAZIONE DEL RISCHIO COMPLESSIVA

Visto l'esito della valutazione dei valori di rischio con riferimento ai singoli rischi di perdita di riservatezza, perdita di integrità, perdita di disponibilità (RID) correlati ai trattamenti necessari per la conduzione degli studi ai sensi dell'art. 110, comma 1, secondo periodo, si ritiene che la valutazione di impatto complessiva individui misure tecniche e organizzative idonee a ricondurre tali rischi ad un livello "basso".