



VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

DPIA (Data Protection Impact Assessment)

Trattamento in esame: Ricerca e sperimentazione clinica¹

Descrizione del trattamento	Attività di Ricerca e sperimentazione clinica, nonché le attività amministrative connesse
Team elaborazione DPIA	Il presente documento è stato elaborato dal team multidisciplinare "Gruppo di Lavoro Area AVEC" che ha concluso i propri lavori in data 27/02/2024 Composizione del Gruppo di Lavoro: Banorri Federica, Del Coco Clara, Descovich Carlo, Domina Rosa, Fiorentini Sabrina, Foglia Maria, Giovannini Tiziana, Iacono Corrado, Infranco Silvia, Maltoni Susanna, Mandrioli Laura, Marani Elisabetta, Pedrazzi Giancarla, Preiti Rosa, Racciatti Eleonora, Santini Luca, Vergnani Paola. All'interno del GdL i DPO Juri Monducci e Manuel Ottaviano hanno fornito consulenza e supporto giuridico
Titolare del trattamento	Azienda USL di Bologna (di seguito Azienda)
RPD/DPO	Manuel Ottaviano
Data di avvio	8 marzo 2023
Data validazione	24 maggio 2024
Frequenza di aggiornamento prevista	Annuale

¹ Trattamento censito nel registro dei trattamenti aziendale

Sommario

DEFINIZIONI E ABBREVIAZIONI	2
1. PREMESSA	4
2. FINALITÀ DEL DOCUMENTO	5
3. AMBITO OGGETTIVO DI APPLICAZIONE	5
4. CATEGORIE DI DATI PERSONALI E BASE GIURIDICA DEL TRATTAMENTO	6
5. TRASPARENZA E DURATA	9
6. CRITERI E METODOLOGIA	10
11. REVISIONE ED AGGIORNAMENTO, CON RIESAME DI CONGRUITÀ CON LE ESIGENZE DI PROTEZIONE DEI DATI - ART 35 GDPR	21
12. APPROVAZIONE DELLA DPIA	21
APPENDICE A - Lista di controllo della congruità del trattamento previsto con le esigenze di protezione dei dati	22
APPENDICE B - Tabella dei rischi afferenti alla DPIA	1
APPENDICE C – Piattaforma REDCap	1
APPENDICE D – Misure di sicurezza	1

DEFINIZIONI E ABBREVIAZIONI

DPIA	Valutazione d'impatto (Data Protection Impact Assessment) - Valutazione ai sensi dell'art. 35 del GDPR che il Titolare del trattamento dei dati è chiamato a svolgere in via preliminare ogni volta che si appresta ad eseguire un trattamento che, per la natura, lo scopo o l'ambito di applicazione potrebbe presentare un elevato rischio specifico per i diritti e le libertà dell'interessato
Ricerca	Qualsiasi indagine con finalità scientifica effettuata in relazione a soggetti umani. La Ricerca può avere ad oggetto ad esempio: medicinali, presidi, dispositivi medici, altro materiale diverso dai precedenti, procedure diagnostiche – terapeutiche, linee guida e percorsi assistenziali, raccolte dati o indagini di materiale biologico. Allo scopo del presente documento, il termine "Ricerca" è sinonimo di "Sperimentazione Clinica", "Studio Clinico", "Indagine Clinica", "Studio", "Progetto di Ricerca" e comprende, tra le altre, le seguenti categorie: 1. studi sia sperimentali che interventistici (ad es. di farmaco/di dispositivo); 2. studi osservazionali (retrospettivi/prospettici).
Attività connesse all'attività di Ricerca	Attività di gestione degli aspetti autorizzativi, normativo-regolatori, amministrativi, contrattualistici e contabili, trattamento dei dati, nonché di esecuzione della Ricerca stessa

GDPR	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). E' il principale testo normativo europeo in materia di protezione dei dati personali
Anonimizzazione	E' una operazione di trattamento che attraverso la de-identificazione trasforma in maniera irreversibile i dati personali in dati anonimi in modo tale che non si possano più attribuire a un interessato specifico
Pseudonimizzazione	Trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile
PI/Sperimentatore	Principal Investigator, Ricercatore responsabile dell'esecuzione della Ricerca. Se la Ricerca è svolta da un gruppo di persone nello stesso centro, lo sperimentatore responsabile del gruppo è definito Sperimentatore principale
Delegation Log	Documento in cui il PI elenca le persone idoneamente qualificate cui ha delegato compiti significativi relativi alla Ricerca di cui è responsabile
N.A.	Non applicabile
CRF	Case Report Form (scheda di raccolta dati utilizzate nell'ambito di studi clinici, survey, gestione di database e progetti di Ricerca), definita come eCRF se in formato elettronico
IOT	Internet of Things, ovvero la possibilità di collegare oggetti di uso quotidiano (elettrodomestici da cucina, auto, termostati, baby monitor, ecc.) a Internet tramite dispositivi incorporati, in modo da realizzare una comunicazione trasparente tra persone, processi e cose
Data Lake	Repository per l'archiviazione di grandi quantità di dati
Open Data	Dati aperti, accessibili a tutti, che possono essere liberamente utilizzati, riutilizzati e ridistribuiti da chiunque
Sistemi di Intelligenza Artificiale	Sistemi sia hardware che software che permettono di dotare le macchine di determinate caratteristiche quali, ad esempio, le percezioni visive, spazio-temporali e decisionali

1. PREMESSA

Presso l'Azienda l'attività di Ricerca è svolta in piena coerenza con le disposizioni dell'ordinamento in materia di protezione dei dati.

Nella norma, per ogni Ricerca è sottoposto all'autorizzazione del Comitato Etico (CE) competente un protocollo corredato di un dettagliato documento informativo per l'acquisizione del consenso informato, ove previsto.

È prevista, anche, la consegna di una Informativa per il 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 degli artt. 110 e 110-bis del Codice privacy.

Coerentemente con il 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" (cfr provvedimento AG per la protezione dei dati personali) per ogni Ricerca è prevista la redazione del progetto denominato, in Area Vasta Emilia Centrale, come "Data Confidentiality and Security Plan" (DCSP). Documento che dà conto della tipologia dei dati trattati e delle operazioni più significative da realizzare col trattamento in questione.

Inoltre, nel caso in cui il protocollo preveda la comunicazione dei dati personali tra i centri partecipanti/collaboranti, di norma 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/Istituto Titolare del trattamento dei dati.

Con riferimento all'attività di valutazione dell'impatto del trattamento di dati personali per finalità di Ricerca, nel corso del 2023, l'Azienda ha avviato una riflessione, congiuntamente alle aziende di Area Vasta AVEC, circa le modalità di svolgimento di dette valutazioni, allo scopo di aggiornare la modalità di conduzione delle DPIA.

Allo scopo, sono stati istituiti due Gruppi di Lavoro composti da:

- I Titolari del Trattamento (Enti del SSR di Area Vasta Emilia Centrale - AVEC);
- Unità operativa DPO (UO DPO);
- Data Protection Officer (DPO);
- Rappresentanti dei Sistemi Informativi;
- UO/infrastrutture di Ricerca aziendali.

Il primo gruppo, nel mese di marzo 2023, ha esaminato la disciplina applicabile, i provvedimenti dell'Autorità Garante (AG) per la Protezione dei Dati Personali maggiormente rilevanti, concludendo i propri lavori con l'adozione di un parere a firma congiunta dei DPO delle Aziende interessate.

Il Gruppo di Lavoro, sopra richiamato, ha condiviso la valutazione secondo la quale il trattamento in esame, dopo essere stato assoggettato all'analisi di rischio, rientra in uno o più casi per i quali è necessaria la conduzione di una DPIA (Data Protection Impact Assessment)

Nell'autunno 2023 gli Enti del SSR di Area Vasta - AVEC hanno promosso un secondo Gruppo di Lavoro, con la finalità di esplorare la possibilità di assoggettare tutta l'attività di Ricerca, ove possibile, ad un'unica valutazione di impatto.

In esito a tale attività valutativa il gruppo ha restituito un riscontro positivo ed ha conferito mandato ad un sottogruppo di lavoro di redigere un testo che poi è stato discusso, integrato e approvato all'unanimità.

Alla luce di quanto sopra esposto, alla conclusione dei lavori del secondo Gruppo di lavoro, in data 26/02/2024, è stata adottata la presente DPIA avente ad oggetto tutta l'attività di Ricerca scientifica e sperimentazione clinica dell'Azienda nelle diverse forme in cui essa si esplica.

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

2. 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).

Con particolare riferimento al trattamento per finalità di Ricerca scientifica, si evidenzia 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 valutarne la necessità e la proporzionalità.

Tale valutazione è necessaria, inoltre, 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.

3. AMBITO OGGETTIVO DI APPLICAZIONE

La presente valutazione ha ad oggetto il trattamento dei dati personali nell'attività di Ricerca, in ogni sua modalità di realizzazione, condotta sull'essere umano.

Tale attività è finalizzata anche al miglioramento delle cure/diagnosi/trattamento dei pazienti, anche attraverso lo sviluppo di nuovi trattamenti o dispositivi medici quali ad esempio i dispositivi IoT direttamente o indirettamente gestiti dai pazienti, dispositivi medici wearable o impiantati, l'adozione o l'innovazione di metodi diagnostici anche attraverso l'utilizzo di tecniche di Intelligenza Artificiale ed ogni altro impiego che con l'utilizzo delle nuove tecnologie possa portare ad un avanzamento della conoscenza teorico-pratico.

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:

1. 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);
2. Trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati afferenti a profili penali e giudiziari come illustrato nell'articolo 10 del GDPR (ex articolo 35, comma 3, lett. b) del GDPR);
3. 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);
4. Trattamenti in cui una violazione dei dati può avere un impatto negativo sulla protezione dei dati stessi, nonché la riservatezza e i diritti o i legittimi interessi degli interessati coinvolti;
5. Trattamenti per i quali la valutazione d'impatto è prevista da disposizioni normative e/o regolamenti.

4. CATEGORIE DI DATI PERSONALI E BASE GIURIDICA DEL TRATTAMENTO

4.1 Le categorie di dati personali

La presente DPIA ha ad oggetto il trattamento dei dati personali degli interessati arruolati negli studi condotti presso l'Azienda 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, persone temporaneamente incoscienti (ad es. in coma, e interdetti/inabilitati).

I Dati personali comprendono:

- Dati anagrafici (sesso, data di nascita e luogo di residenza).
- 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, dispositivi, campioni biologici e dati genetici.

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 coinvolti nel progetto di Ricerca, tra i quali dati anagrafici, dati di contatto (indirizzo e-mail) e i log delle attività svolte.

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.

4.2 La base giuridica

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 o nazionale. Tale trattamento dev'essere proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, in conformità dell'articolo 89, paragrafo 1 del Regolamento (art. 9, par. 2, lett. j) del Regolamento).

Nel solco dello spazio normativo definito da tale ultima disposizione, il legislatore italiano ha introdotto - integrando a livello nazionale il GDPR - la medesima disposizione previgente del Codice privacy che riguarda la Ricerca medica, biomedica ed epidemiologica, ovvero l'art. 110.

L'art. 110 dispone 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 e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento".

La base giuridica, quindi, per finalità di Ricerca e sperimentazione clinica è costituita da:

- art. 9, par. 2 lettera a) del GDPR;
- art. 9, par. 2 lettera j) del GDPR
- art. 110 del Codice Privacy;
- art. 110-bis del Codice Privacy.

È nel consenso (art. 9, par. 2 lettera a) del GDPR), dunque, che è possibile rinvenire la base giuridica del trattamento di dati per finalità di Ricerca scientifica, seppure siano previste alcune eccezioni.

In effetti, il consenso dell'interessato non è necessario (secondo l'art. 9, par. 2, lettera j) del GDPR e l'art. 110 del Codice Privacy) quando la Ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione Europea.

Negli altri casi, quando non è possibile acquisire il consenso degli interessati (coerentemente con il 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"), è documentata, nel progetto di Ricerca, nel DCSP, la 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, tra le quali in particolare:

1. i 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. i 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 dell'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.

Agli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS), pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta rispetto alla Ricerca, è consentito il riuso dei dati dei propri assistiti in assenza del consenso (dall'art. 110-bis del Codice Privacy).

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

4. Regole Deontologiche per trattamenti a fini statistici o di Ricerca scientifica (Provvedimento dell'Autorità Garante del 19 dicembre 2018 n. 515).

5. 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"

6. Regolamento Regione Emilia-Romagna (RER) n. 1/2014 Allegato B.

5. TRASPARENZA E DURATA

Come accennato in premessa, la presente Valutazione d'impatto è oggetto di pubblicazione sul sito web istituzionale nella sezione privacy dedicata all'attività di Ricerca.

Accanto al presente documento 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).

L'informativa viene fornita all'interessato (ivi compresi genitori/tutori/amministratori di 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 e i tempi di trattamento e conservazione dei dati.

In materia di trasparenza, l'attività di Ricerca si conforma alle indicazioni del Consiglio di Stato (Sez. VI), il quale nella pronuncia del 13 dicembre 2019 n. 8472 ha dichiarato che "dal diritto sovranazionale emergono tre principi, da tenere in debita considerazione nell'esame e nell'utilizzo degli strumenti informatici:

- il principio di conoscibilità, per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino ed in questo caso a ricevere informazioni significative sulla logica utilizzata;
- il principio di non esclusività della decisione algoritmica;
- il principio di non discriminazione algoritmica, secondo cui è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche."

Inoltre, con riferimento agli studi ed alle sperimentazioni nei quali è previsto l'utilizzo di Intelligenza Artificiale, coerentemente con il parere congiunto del Comitato Europeo per la Protezione dei Dati e il Garante Europeo, n. 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (legge sull'Intelligenza Artificiale del 21 aprile 2021), è valorizzato un approccio graduato e adattato al rischio concreto connesso alle attività. Ovvero, sono concretamente valutati i rischi per i diritti e le libertà fondamentali degli interessati derivanti dall'utilizzo di tali strumenti, alla luce della considerazione per la quale esiste una sostanziale differenza tra le modalità con cui attività, quali generare contenuti, fare previsioni o adottare decisioni in maniera automatica, sono svolte dagli esseri umani. Non è previsto in alcuna Ricerca l'affidamento in via esclusiva alle macchine del compito di prendere decisioni sulla base di dati senza la sorveglianza (o supervisione) umana, al fine di

assicurare il rispetto del diritto di non essere assoggettato a una decisione basata esclusivamente su un trattamento automatizzato.

6. CRITERI E METODOLOGIA





7.1 Valutazione preliminare dell'utilizzo dei dati

7.1.1 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.

7.1.2 Chi avrà accesso ai dati?

---omissis---

7.1.3 In che modo i dati verranno eventualmente trasferiti/comunicati a soggetti terzi?

---omissis---

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.

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

---omissis---

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



8.1 Tecnologie utilizzate

8.1.1 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?

Il trattamento in questione prevede l'utilizzo di tecnologie che possono ridurre o provocare un potenziale rischio per gli interessati:

---omissis---

8.2 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.

8.2.3 Verranno utilizzati nuovi o significativamente modificati requisiti di autentica di identità, che possono risultare intrusivi od onerosi per il soggetto interessato?

---omissis---

8.3 Coinvolgimento di altre strutture

8.3.1 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 (cfr. punto 7.1.3, per le attività di comunicazione e di trasferimento dei dati).

8.4 Modifiche alle modalità di trattamento dei dati

8.4.1 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.

8.4.2 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 formati per finalità di cura, quindi non modificabili, diversamente da quanto accade negli studi prospettici dove i dati vengono trattati su CRF predisposte ad hoc, sempre tenendo conto dei principi generali che regolano il corretto trattamento dei dati personali.

8.4.3 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.

8.5 Modifiche alle procedure di trattamento dei dati

8.5.1 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.

8.5.2 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 conosciuti attraverso l'informativa e fanno riferimento al protocollo di Ricerca o sono determinati dal massimario di scarto.

8.5.3 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. Si richiama per opportuno riferimento il punto 6.2.3 relativamente alla comunicazione o al trasferimento dei dati.

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

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

---omissis---

8.7 Si prevede di effettuare una consultazione istituzionale?

È stato effettuato un confronto sia all'interno alla Azienda/Istituto sia nell'ambito dell'Area Vasta Emilia Centrale attraverso l'avvio di due Gruppi di Lavoro e un sottogruppo, nei quali sono state condivise le linee strategiche generali e specifiche per la conduzione della presente DPIA.

All'interno del percorso di cui sopra, sono stati esaminati gli elementi di diritto e le pronunce dell'Autorità Garante al fine di predisporre uno schema-tipo di valutazione d'impatto. In esito a tale attività è stata licenziata una DPIA che ogni Azienda/Istituto aderente all'AVEC utilizzerà per l'adozione della propria valutazione d'impatto circa le attività di Ricerca.

Dal punto di vista della governance, presso ogni Azienda/Istituto sono in uso percorsi tesi alla regolamentazione delle attività di Ricerca e di sperimentazione.

Il percorso istruttorio individua in maniera puntuale il riparto delle funzioni attribuite.

La costituzione dei predetti Gruppi di Lavoro ha esplicitato la strategia di consultazione adottata dal Titolare, secondo la quale sono stati messi a fattor comune gli elementi caratterizzanti il trattamento. Nel dettaglio, si è svolto un confronto profondo tra i DPO, le funzione privacy dell'Azienda/Istituto, le ICT e i componenti delle U.O./Uffici/Infrastrutture Ricerca.

8.7.1 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 art. 13 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.).

9

**ESITO
DELL'ANALISI
PRELIMINARE
DEI RISCHI**

9.1 Identificazione preliminare dei rischi

La tabella seguente illustra i principali rischi afferenti al trattamento dei dati e che sono stati identificati in fase di valutazione preliminare.

---omissis---	---omissis---	---omissis---
---omissis---	---omissis---	---omissis---
---omissis---	---omissis---	---omissis---
---omissis---	---omissis---	---omissis---
---omissis---	---omissis---	---omissis---
---omissis---	---omissis---	---omissis---
---omissis---	---omissis---	---omissis---

9.2 Decisione su come procedere

Tenendo conto della tipologia di trattamento e in conformità delle indicazioni previste all'articolo 35, paragrafo 3 del Regolamento Generale sulla protezione dei dati – Regolamento (UE) 2016/679 – GDPR, è necessario effettuare la DPIA sul trattamento della Ricerca in ogni sua declinazione.

9.3 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, come parte di questa DPIA, 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.

10

CONTENUTI
ANALITICI
DELLA DPIA



10.1 Descrizione analitica delle operazioni di trattamento, con indicazione delle finalità perseguite dal Titolare del Trattamento

I dati personali e quelli appartenenti a particolari categorie degli interessati (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, nel DCSP e nel protocollo della Ricerca.

10.2 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.

10.3 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.

10.4 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.

Dette misure prevedono disposizioni in materia di sicurezza fisica e logica dei sistemi elencati all'Appendice D.

Di seguito vengono, inoltre, descritte le misure tecniche e organizzative adottate per mitigare i rischi per i diritti e le libertà degli Interessati.

10.5 Elenco dettagliato delle salvaguardie, delle misure di sicurezza e dei meccanismi adottati per garantire la protezione dati personali, come ad esempio la pseudonimizzazione, oppure la crittografia, al fine di dimostrare la congruità con il regolamento, tenendo conto dei diritti e dei legittimi interessi degli interessati ed altre persone coinvolte

---omissis---

10.6 Misure organizzative

---omissis---

10.7 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 REDCap) con accesso limitato al PI e ai suoi delegati tramite credenziali personali.

---omissis---

10.8 Indicare le salvaguardie previste se i dati personali sono trasferiti o comunicati a paesi terzi

Vedasi il punto 8.6.1.

10.9 Eventuale coinvolgimento del DPO

Il percorso che ha condotto alla redazione di un modello unico di DPIA è stato proposto dal sottogruppo indicato in premessa, che preliminarmente ne ha approfondito gli aspetti di natura metodologica e tecnico-giuridica e successivamente ha elaborato il documento presentandolo quale esito dei lavori ai Gruppi di Lavoro.

11. REVISIONE ED AGGIORNAMENTO, CON RIESAME DI CONGRUITÀ CON LE ESIGENZE DI PROTEZIONE DEI DATI - ART 35 GDPR

Il riesame di congruità del presente documento è condizionato ad eventuali modifiche organizzative e normative che possono determinarsi nel corso della Ricerca.

11.1 Data entro la quale deve essere condotto il riesame di congruità

La revisione della DPIA verrà effettuata tempestivamente nei casi specifici in cui è necessaria un'azione correttiva o di miglioramento delle modalità di trattamento.

Il riesame 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.

Anche in questa fase verrà chiesto il parere del DPO.

12. APPROVAZIONE DELLA DPIA

12.1 da parte della direzione

Il presente documento è stato sottoposto dalla Direzione al DPO che ha rilasciato parere favorevole.

APPENDICE A - Lista di controllo della congruità del trattamento previsto con le esigenze di protezione dei dati

---omissis---	---omissis---
1. ---omissis---	---omissis---
2. ---omissis---	---omissis---
3. ---omissis---	---omissis---

4. ---omissis---	---omissis---
5. ---omissis---	---omissis---
6. ---omissis---	---omissis---
7. ---omissis---	---omissis---
8. ---omissis---	---omissis---
9. ---omissis---	---omissis---
10. ---omissis---	---omissis---
11. ---omissis---	---omissis---
---omissis---	- ---omissis---

APPENDICE B - Tabella dei rischi afferenti alla DPIA

---omissis---	---omissis---			---omissis---	---omissis---		
	--- omissis-- -	---omissis---	--- omissi s---		Impatto	Probabilità	Rischio
---omissis---	--- omissis-- -	---omissis---	--- omissi s---	---omissis---	--- omissis---	---omissis-- -	--- omissis- --
---omissis---	--- omissis-- -	---omissis---	--- omissi s---	---omissis---	--- omissis---	---omissis-- -	--- omissis- --
---omissis---	--- omissis-- -	---omissis---	--- omissi s---	---omissis---	--- omissis---	---omissis-- -	--- omissis- --
---omissis---	--- omissis-- -	---omissis---	--- omissi s---	---omissis---	--- omissis---	---omissis-- -	--- omissis- --
---omissis---	--- omissis-- -	---omissis---	--- omissi s---	---omissis---	--- omissis---	---omissis-- -	--- omissis- --
---omissis---	--- omissis-- -	---omissis---	--- omissi s---	---omissis---	--- omissis---	---omissis-- -	--- omissis- --
---omissis---	--- omissis-- -	---omissis---	--- omissi s---	---omissis---	--- omissis---	---omissis-- -	--- omissis- --

LEGENDA

Probabilità (P)		
1	molto bassa	accade solo in circostanze eccezionali ($P < 5\%$)
2	bassa	è improbabile che accada ($5\% < P < 20\%$)
3	media	può accadere in un certo numero di casi ($20\% < P < 50\%$)
4	alta	avviene in una buona parte dei casi ($50\% < P < 75\%$)
5	molto alta	avviene nella maggior parte dei casi ($P > 75\%$)

	Probabilità (P)				
Impatto (I)	molto bassa (1)	bassa (2)	media (3)	alta (4)	molto alta (5)
molto bassa (1)	1	2	3	4	5
bassa (2)	2	4	6	8	10
media (3)	3	6	9	12	15
alta (4)	4	8	12	16	20
molto alta (5)	5	10	15	20	25

--- omissis- --	---omissis---	---omissis---
--- omissis- --	---omissis---	---omissis---
--- omissis- --	---omissis---	---omissis---
--- omissis- --	---omissis---	---omissis---

APPENDICE C – Piattaforma REDCap

Scheda sintetica della DPIA condotta sulla piattaforma REDCap in data 28/01/2022

Premessa

La piattaforma REDCap (Research Electronic Data Capture), costituita nel 2004 dalla Vanderbilt University, permette di creare, in modo gratuito e sicuro, schede di raccolta dati elettroniche a supporto di varie fasi di un progetto di Ricerca: creare la scheda di raccolta dati (eCRF), monitorare la qualità del dato inserito (ad es. formato, range, coerenza con campi complementari), creare report automatici per il monitoraggio della Ricerca, esportare i dati raccolti in formati adatti a successive elaborazioni statistiche.

Elementi caratteristici di REDCap

La piattaforma REDCap permette di:

- progettare, costruire e mettere in opera database per raccolta dati di studi mono o multicentrici,
- di raccogliere dati su un server privato, accessibile esclusivamente tramite account personale,
- gestire la qualità del dato configurando il sistema in modo tale che vi siano dei controlli sui dati inseriti (formato, range ecc.),
- creare query automatiche e manuali per il monitoraggio della Ricerca,
- esportare i dati raccolti nei formati utili per le elaborazioni statistiche.

Raccolta dati

Di norma i dati sono forniti direttamente dal soggetto interessato (o da soggetti che esercitano nei confronti dell'interessato la patria potestà, o rivestono la qualifica di tutori) o da soggetti da 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 approvato dal Comitato Etico (CE).

Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi previsti, 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.

I dati possono pervenire all'Azienda/Istituto anche su comunicazione di soggetti terzi, con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi.

Non verranno inseriti dati personali dell'interessato ma esclusivamente un ID univoco associato all'anagrafica.

L'associazione ID/anagrafica è gestita e archiviata su sistemi informatici differenti ma altrettanto sicuri sotto la responsabilità del PI.

Accesso ai dati

---omissis---

Analisi dei rischi

---omissis---

Conclusione

L'impiego di REDCap, per le esigenze dell'attività di Ricerca riguarderà tutte le strutture dell'Azienda, ad eccezione dei casi nei quali i partecipanti alla Ricerca multicentrica decidano di servirsi di altro applicativo.

La piattaforma, inizialmente adottata da ogni singola Azienda, è stata successivamente sottoposta ad un percorso interAziendale, unitario, di valutazione. In tale ambito è stata realizzata l'armonizzazione degli originari documenti.

Il percorso ha permesso di condividere le scelte di sviluppo e applicazione del sistema approfondendo in modo specifico gli aspetti di interconnessione e integrazione del sistema con altri applicativi di gestione dei flussi informativi, in uso nelle aziende.

Il percorso, di ambito AVEC, è stato guidato dalla UO DPO inter Aziendale ed ha prodotto:

- La creazione e coordinamento di un gruppo di lavoro multidisciplinare formato da professionisti tecnici e sanitari delle Aziende coinvolte;
- La realizzazione di contributi di tipo metodologico, giuridico e tecnico;
- Una valutazione d'impatto unica, approvata poi dalle singole aziende titolari del trattamento.

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.

Il DPO dopo aver valutato che il trattamento si colloca in una gradazione di rischio *Basso*, quindi, tale da non attivare il procedimento di consultazione preventiva all'Autorità Garante, ha espresso parere favorevole all'utilizzo della piattaforma REDCap, pur tuttavia, indicando alcune raccomandazioni in ordine alle misure di sicurezza tecniche ed organizzative adottate, in termini di:

- modifiche del contesto organizzativo o delle finalità del trattamento,
- tipologia di dati personali trattati,
- modalità di raccolta dei dati personali,
- combinazioni di dati provenienti da fonti differenti,
- destinatari e/o trasferimento di dati in Paesi terzi,
- presenza di nuove minacce,
- modifica ai sistemi informativi a supporto del trattamento,
- modifiche di contromisure esistenti,
- nuovi scenari di rischio,
- attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali.

APPENDICE D – Misure di sicurezza

---omissis---