SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Bologna
IRCCS Istituto di Ricovero e Cura a Carattere Scientifico

FRONTESPIZIO PROTOCOLLO GENERALE

AOO: AOPSO_BO

REGISTRO: Protocollo generale

NUMERO: 0022050

DATA: 24/05/2024 17:00

OGGETTO: Risposta a richiesta di parere su Valutazione d'impatto sul trattamento dati personali (DPIA) ai sensi dell'art. 35 del GDPR relativa alle attività di ricerca e sperimentazione clinica

SOTTOSCRITTO DIGITALMENTE DA:

Manuel Ottaviano

CLASSIFICAZIONI:

- [03-01]

DOCUMENTI:

File	Firmato digitalmente da	Hash
PG0022050_2024_Lettera_firmata.pdf:	Ottaviano Manuel	798F7486E7FC37E2515C1F1FC50618F8E81F248D9B5EB63254C81E0E6484BE15
PG0022050_2024_Allegato3.pdf:		4EB867E9CE3100840F60D13D4CCBC3282F2F785F68835C89E894E95E90D1CE56
PG0022050_2024_Allegato1.pdf:		91242FEFE327C92AA98991F0DF43A2EF724B94594F738145F2946B3FE86F06E5
PG0022050_2024_Allegato2.pdf:		E88CB8512E1993A284353773A6B2920CD1D4CC0564866F137AE22CA1231B87EC

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA

Azienda Ospedaliero-Universitaria di Bologna (IRCCS)
Azienda Unità Sanitaria Locale di Bologna - ISNB (IRCCS)
Azienda Unità Sanitaria Locale di Imola
Istituto Ortopedico Rizzoli di Bologna (IRCCS)
Montecatone Rehabilitation Institute

DATA PROTECTION OFFICER

UOC AFFARI GENERALI E RAPP.
CON UNIVERSITA'

SS CLINICAL TRIAL CENTER (CTC)

DIREZIONE GENERALE

OGGETTO: Risposta a richiesta di parere su Valutazione d'impatto sul trattamento dati personali (DPIA) ai sensi dell'art. 35 del GDPR relativa alle attività di ricerca e sperimentazione clinica

In riscontro alla richiesta di parere, prot. 17066 del 19/04/2024, sulla DPIA relativa al trattamento dei dati effettuato nell'attività di ricerca e sperimentazione clinica, si rilascia il parere allegato.

Il giudizio favorevole è rilasciato in forma congiunta con il Responsabile della Protezione dei Dati personali delle Aziende Sanitarie di Ferrara, anche alla luce dei lavori del GdL Ricerca istituito in area AVEC.

E' opportuno che nella fase di rilascio del Nulla Osta da parte del Direttore Generale sia inserito il riferimento al n. di protocollo di cui alla presente nota.

Ai fini della completezza della documentazione di studio, si rammenta l'importanza:

- della compilazione del Data Confidentiality Security Plan (DCSP) specifico per ogni studio;
- dell'informativa e consenso al trattamento dei dati;
- degli eventuali M/DTA;
- della eventuale definizione dell'architettura del trattamento, ivi inclusi gli accordi tra le parti.

Distinti saluti

Responsabile procedimento:
Manuel Ottaviano

Firmato digitalmente da:

Manuel Ottaviano

Dott. Manuel Ottaviano
Data Protection Officer

Azienda Ospedaliero - Universitaria di Bologna (IRCCS)
Via Albertoni, 15 - 40138 Bologna
T. +39.051.214.1111 - F. +39.051.636.1202
Cod. Fisc. 92038610371 - P. Iva 02553300373

Parere dei Responsabili della Protezione dei Dati personali sulla valutazione d'impatto relativa al trattamento di Ricerca e sperimentazione clinica.

Sommario

1. Descrizione del trattamento e del servizio

Premessa

Il Titolare del trattamento ha ritenuto opportuno assoggettare tutta la propria attività di ricerca e sperimentazione clinica ad una valutazione unitaria di impatto, invece di compiere tale attività per ogni singolo progetto di studio.

Detto documento, pur avendo carattere generico e, pertanto, applicabile ad ogni trattamento del Titolare, alla luce dell'analisi del rischio svolta, esamina puntualmente le misure di sicurezza fisica e logica applicabili ed idoneea mitigare i rischi per i diritti e le libertà fondamentali degli interessati, le quali saranno applicate ad ogni progetto di ricerca iniziato in seguito alla redazione del documento in oggetto.

Ogni studio prevede la predisposizione di una Informativa per il trattamento dei dati personali dedicata, redatta ai sensi degli artt. 13 e 14 del GDPR. 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.

È prevista la stipula di dettagliati Data/Material Transfer Agreement per studi multicentrici.

È altresì prevista la compilazione del Data Confidentiality and Security Plan (DCSP) che effettua una fotografia del progetto di studio ed esamina puntualmente la tipologia dei dati da trattare e le operazioni di trattamento, l'architettura istituzionale del trattamento, le misure di sicurezza, il periodo di conservazione dei dati, le ragioni ostative alla raccolta del consenso ed informazioni specifiche nel caso del trattamento di dati genetici.

Il Protocollo di studio è sottoposto all'autorizzazione del Comitato Etico di riferimento corredato di un dettagliato documento informativo per l'acquisizione del consenso informato al trattamento dei dati personali.

L'avvio dello studio è subordinato al rilascio del nulla osta da parte del Direttore Generale, ai sensi dell'art. 7 della Legge Regionale E.R. n. 9 del 2017, della struttura sanitaria in cui è condotta l'attività, affinché sia garantita anche l'assenza di pregiudizi per l'attività assistenziale.

1.1 Finalità del trattamento.

La valutazione d'impatto, oggetto del presente parere del Responsabile della Protezione dei Dati, prende in esame il trattamento dei dati personali nell'attività di ricerca e di sperimentazione clinica condotta sull'uomo, sia sano sia malato.

L'attività è finalizzata al miglioramento delle cure dei pazienti 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.

1.2 Categoria di dati trattati

Oggetto del trattamento sono i dati così come definiti dall'art. 4 del GDPR e nello specifico:

- dati personali;
- dati genetici;
- dati biometrici;
- dati relativi alla salute.

1.3 Soggetti interessati

I soggetti interessati dal trattamento sono:

- soggetti tra gli aventi diritto alle prestazioni assistenziali del titolare o di altro titolare;
- pazienti che hanno ricevuto o ricevono dal Titolare del trattamento prestazioni sanitarie nell'ambito della normale pratica clinica; tra i quali: minori, soggetti temporaneamente incapaci di esprimere la propria volontà poiché in situazioni di fragilità clinica o decadimento cognitivo, incoscienti (per es. in coma) e/o interdetti/inabilitati;
- soggetti i cui dati sono stati trasmessi al Titolare da altri partner di ricerca

L'attività in esame potrebbe riguardare anche il trattamento dei dati personali, degli operatori coinvolti nel progetto di studio/sperimentazione, quali a mero titolo di esempio: dati anagrafici, dati di contatto (indirizzo e-mail) e i dati di log delle attività svolte.

1.4 Base giuridica

La base giuridica per le finalità di ricerca e sperimentazione clinica è costituita:

- dall'art. 9, par. 2 lettera a) e lettera j del GDPR;
- dagli artt. 110 e 110 bis del Codice Privacy.

Nell'ipotesi in cui non sia possibile acquisire il consenso dell'interessato, sarà documentata nel progetto di ricerca, la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulti impossibile o implica uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca (l'impossibilità organizzativa di acquisire il consenso è accertata in presenza di tre tentativi infruttuosi di raccolta, validamente sostanziata).

1.5 Modalità di raccolta dei dati

I dati oggetto del trattamento vengono raccolti attraverso varie fonti a seconda della tipologia dello studio da realizzare (direttamente dagli interessai, dalle cartelle cliniche; dai database; dalle biobanche, ecc.).

1.6 Accesso ai dati: autorizzati al trattamento

L'accesso ai dati trattati è riservato, per determinate attività, ai soggetti di seguito indicati (ognuno dei quali è stato opportunamente autorizzato al trattamento dei dati ex art. 29 GDPR):

- per le attività di ricerca e di sperimentazione clinica: PI e soggetti compresi nel delegation log.
- per le attività di manutenzione dei sistemi informativi: servizio ICT ed eventuali fornitori.
- per le attività di vigilanza: Funzione Privacy aziendale e il DPO.

1.7 Aggiornamento, archiviazione e cancellazione dei dati

Nel rispetto del principio di "esattezza" e di "limitazione della conservazione", i dati relativi agli studi saranno aggiornati in funzione delle attività svolte, archiviati in forma aggregata per il tempo definito in ogni protocollo di studio ed eliminati al termine temporale anch'esso definito nel protocollo, nei solo casi previsti dall'informativa,studio specifica, redatta ai sensi dell'art. 13 GDPR i dati possono essere anonimizzati e conservati per finalità ulteriori.

1.8 Privacy by Design e Privacy by Default

All'interno della valutazione d'impatto, il Titolare garantisce che il trattamento è conforme al RGPD, in quanto è stato progettato nel rispetto dei principi di *privacy by design* e *by default*; il livello di sicurezza e dei dati personali è mantenuto adeguato al rischio mediante un processo di assessment di sicurezza "in continuo". È stata implementata una strategia di difesa multidimensionale per una maggiore protezione e gestione dei dati.

In ossequio al principio di minimizzazione verranno raccolti solo dati e informazioni necessarie ai fini della ricerca e successivamente verranno applicate procedure di pseudonimizzazione applicando un codice alfanumerico o numerico..

Il che consente che i dati personali non possano essere più associabili a un soggetto specifico senza l'utilizzo di informazioni aggiuntive, che solo il PI conosce. Si attua quindi una misura di sicurezza idonea a ridurre il livello di rischio.

I dati clinici e i referti delle indagini eseguite sono registrati su eCRF e gestiti, di norma, attraverso l'applicativo REDCAP. I dati possono altresì essere gestiti con altri strumenti, qualora la specificità del progetto lo preveda, ma in ogni caso l'accesso è permesso al PI che vi accede attraverso ID/password.

1.9 Comunicazione dei dati

La comunicazione ed il trasferimento dei documenti contenenti dati sanitari avvengono solo tramite PEC, allegando i documenti in formato criptato. La chiave di decriptazione viene inviata in una diversa ed ulteriore comunicazione.

Inoltre, le comunicazioni potranno avvenire attraverso piattaforme Cloud del titolare o rese disponibili da altri partner di progetto.

2. Necessità della valutazione d'impatto ex. art. 35 GDPR

La valutazione d'impatto, come definita nel documento WP 248, rev. 01 dal Gruppo di lavoro articolo 29 per la protezione dei dati, "*è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli*". In altri termini può essere vista come strumento utile al Titolare per dimostrare di aver adottato misure tecniche e organizzative adeguate a garantire che il trattamento venga effettuato in linea con il GDPR e quindi per dimostrare la conformità al principio di responsabilità del titolare previsto dall'art. 24 del GDPR.

Tale adempimento viene descritto come necessario dall'art. 35 del GDPRquando il trattamento in oggetto "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*". Per chiarire meglio la prescrizione astratta della normativa, il Gruppo di lavoro articolo 29 per la protezione dei dati, nel citato documento WP 248, rev. 01, ha stilato un elenco esemplificativo di 9 tipologie di trattamenti che necessitano della valutazione d'impatto.

Anche l'Autorità Garante per la protezione dei dati personali ha emanato, a sua volta, con il Provvedimento n. 467 dell'11 ottobre 2018, l'elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto contenente 12 tipologie di trattamento che necessitano del citato adempimento.

La medesima Autorità Garante, in una infografica riassuntiva[1] in merito alla valutazione d'impatto chiarisce le ipotesi nelle quali è necessario effettuare tale adempimento riprendendo i 9 punti elencati dal citato documento WP 248, rev. 01 e ritenendoli criteri utili a individuare i casi in cui il trattamento possa presentare un rischio elevato per i diritti e le libertàdelle persone fisiche.

Nella seguente tabella vengono indicati i 9 criteri marcando i fattori che hanno fatto ritenere necessaria la valutazione d'impatto al Titolare del trattamento.

CRITERI PER INDIVIDUARE RISCHIO ELEVATO WP 248, rev. 01	RISCHIO PRESENTE (✓) NON PRESENTE (X) nel trattamento oggetto di valutazione
trattamenti valutativi o di *scoring*, compresa la profilazione	✓

[1] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7185457

decisioni automatizzate che producono significativi effetti giuridici	X
monitoraggio sistematico	✓
trattamento di dati sensibili, giudiziari o di natura estremamente personale	✓
trattamenti di dati personali su larga scala	✓
combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale	✓
dati relativi a soggetti vulnerabili (minori e/o pazienti e/o dipendenti)	✓
utilizzi innovativi o applicazione di nuove soluzioni tecnologiche organizzative	✓
trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	X

L'attività di trattamento considerati la natura, l'oggetto, il contesto e le finalità, 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, ed è per questo che il Titolare del trattamento ha correttamente ritenuto opportuno effettuare una valutazione di impatto per descrivere le misure adottate per attenuare i rischi connessi con l'utilizzo del servizio in oggetto sino a renderli medio-bassi.

Invero, il trattamento in esame, dopo essere stato assoggettato all'analisi di rischio, rientra in uno o più casi sottoelencati, per i quali è necessaria la conduzione di una DPIA:

- 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 sull'interessato (ex articolo 35, paragrafo 3, lett. a) del GDPR);
- trattamento, su larga scala, di categorie particolari di dati personali;
- altre attività di trattamento che siano inseriti nell'elenco pubblico dell'autorità garante nazionale e che richiedono specificamente lo sviluppo di una DPIA;
- trattamenti in cui una violazione dei dati può avere un impatto negativo sulla protezione dei dati stessi, nonché suidiritti degli interessati coinvolti;
- trattamenti per i quali la valutazione d'impatto è prevista da disposizioni normative e/o regolamenti.

3. Misure di sicurezza adottate per rendere il rischio residuo tollerabile

All'interno della valutazione d'impatto predisposta dal Titolare del trattamento vengono descritte le seguenti misure di sicurezza volte a rendere il rischio residuo medio-basso:

- CRITTOGRAFIA DELLE PASSWORD: le password degli utenti vengono memorizzate in formato criptato, ovvero, utilizzando algoritmi e altre tecniche per avere un'elevata resistenza agli attacchi, anche di forza bruta e di dizionario.

- CRITTOGRAFIA DEI DATI IN TRANSITO:qualora sia necessario procedere alla comunicazione o trasferimento dei dati, essi vengono crittografati durante la trasmissione tra le diverse componenti del sistema, anche quando vengono inviati i dati da un'applicazione web a un server.

- PSEUDONIMIZZAZIONE: a ciascun paziente arruolato nello studio/ricerca viene assegnato un ID alfa-numerico/numerico. La corrispondenza tra tale ID e l'identificativo univoco ospedaliero del paziente è conservata all'interno di uno schema separato e gestito da personale autorizzato dal Titolare.

- CONTROLLO DEGLI ACCESSI LOGICI: la sicurezza degli accessi nella componente server è assicurata attraverso privilegi di accesso relativi alle singole funzioni erogabili dal sistema rispetto ad ogni dataset in esso contenuto. Ovvero, vengono collegati a specifici ruoli coerentemente con il delegation log. Inoltre, l'autenticazione può essere gestita utilizzando l'interfaccia L-Dap, oppure, può essere configurata con una two-factor authentication (nome utente e password).

- TRACCIABILITÀ: la tracciabilità dei dati viene garantita attraverso l'utilizzo di log per registrare le operazioni effettuate sul database da parte degli utenti o dei processi autorizzati; l'utilizzo di tabelle di log per registrare la data e l'ora di creazione, modifica o cancellazione dei record del database, l'utilizzo di controlli di qualità per valutare la completezza, l'accuratezza, la consistenza e la validità dei dati.

- ARCHIVIAZIONE: i tempi di archiviazione dei dati sono definiti nel protocollo di studio o dal massimario di scarto qualora si preveda l'archiviazione di tali dati in forma anonima.

- CONTROLLO DEGLI ACCESSI FISICI:l'accesso fisico ai locali che ospitano i server, viene regolato dal Referente privacy/PI responsabile ICT, attraverso misure che possono prevedere a seconda dei casi: accesso con badge, area video sorvegliata, ecc.

- MINIMIZZAZIONE DEI DATI: nell'ambito dell'attività di ricerca e sperimentazione clinica vengono trattati esclusivamente i dati indicati nel dataset della eCRF dello studio, inoltre, in tutti i casi in cui viene raccolto un consenso specifico per la realizzazione dello studio tale informazione viene utilizzata per selezionare solo pazienti con consenso.L'accesso all'identificativo univoco ospedaliero del paziente, memorizzato come descritto alla sezione "pseudonimizzazione", è permesso solo ove strettamente necessario ad un numero limitato di soggetti

- VULNERABILITÀ: viene assicurata la protezione relativamente alle vulnerabilità software attraverso l'attuazione di una manutenzione ordinaria per l'applicazione di eventuali patch di sicurezza. La protezione relativamente alle possibili vulnerabilità software è garantita attraverso una costante attività di formazione del personale autorizzato al trattamento dei dati; sviluppo di procedure di pseudonimizzazione; aggiornamento annuale del sistema; piano di risposta agli incidenti.

- LOTTA CONTRO IL *MALWARE*: è previsto il controllo periodico della sicurezza dei server verificando che l'antivirus sia presente, aggiornato e funzionante e che non ci sia un traffico di rete anomalo in uscita dalla data di ultima verifica.

- *BACKUP*: il Titolare è responsabile delle procedure di backup: sono impostati backup giornalieri e retention di almeno 30 giorni su server separati.

- MANUTENZIONE: la manutenzione del server fisico è demandata al personale del servizio ICT, autorizzato al trattamento e adeguatamente istruito .

- SICUREZZA DEI CANALI INFORMATICI: il firewall è adeguatamente configurato dal

personale ICT del Titolare

- TRACCIABILITÀ SUI SISTEMI: gli accessi per le attività sistemistiche vengono tracciati su un sistema unico gestito in dominio aziendale; le credenziali ai sistemi sono individuali e profilate secondo quanto definito nelle *policy* di dominio.

- SICUREZZA DELL'*HARDWARE*: le configurazioni di sicurezza relative all'hardware sono demandate al personale ICT del Titolare

- PROTEZIONE CONTRO FONTI DI RISCHIO NON UMANE: la presenza di backup giornalieri e retention di almeno 30 giorni su server separati è utile per evitare la perdita di dati.

- ULTERIORI MISURE DI SICUREZZA INFRASTRUTTURALI ED ORGANIZZATIVE: gestione delle postazioni e dei dispositivi aziendali; designazione del responsabile del trattamento e indicazione delle istruzioni, policy in materia di protezione dei dati; gestione delle policy in materia di protezione dei dati; gestione dei rischi; policy per la gestione degli incidenti di sicurezza e le violazioni dei dati personali; gestione del personale; gestione dei terzi che accedono ai dati; vigilanza sul rispetto della prescrizione della normativa sulla protezione dei dati.

4. Valutazione finale del Responsabile della protezione dei dati (RPD)

Come detto in premessa, il Titolare del trattamento ha ritenuto opportuno assoggettare tutta la propria attività di ricerca e sperimentazione clinica ad una valutazione unitaria di impatto, anziché compiere tale attività per ogni singolo progetto di studio.

Il documento, pertanto, deve avere necessariamente carattere generico, dovendo essere valido per ogni attività di studio intrapresa; tuttavia, si segnala che laddove gli studi e le ricerche dovessero presentare delle peculiarità rispetto al modello base, la valutazione di impatto dovrà essere condotta .

Ciò detto, lo scrivente Responsabile, dopo aver valutato positivamente le misure di sicurezza adottate dal Titolare del trattamentoe dopo aver analizzato la valutazione di impatto in cui viene espressamente enucleato come, attraverso l'utilizzo delle citate misure di sicurezza, il rischio di esposizione a eventuali accessi illegittimi ai dati, modifiche indesiderate ai dati e perdita di dati venga limitato e reso di valore medio-basso, esprime parere favorevole all'implementazione nell'attività di ricerca e di sperimentazione clinica condotta sull'uomo.

In particolare, il rischio di distruzione e perdita del datoviene reso minimo dall'implementazione delle misure di: backup, monitoraggio, formazione.

Il rischio di accesso ai dati da parte di un soggetto non autorizzato viene mitigato, invece, da: accesso ai dati riservato; pseudonimizzazione; gestione postazioni; controllo degli accessi fisici; sicurezza dei documenti cartacei; sicurezza dei canali informatici; gestione delle politiche di tutela della privacy; formazione; stratificazione delle autorizzazioni; password rinforzata per accedere ai dati.

Pertanto, ai sensi dell'art. 32 del GDPR, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, oggetto del presente parere, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, le misure tecniche ed organizzative predisposte dal titolare, dopo attenta a analisi e valutazione,a parere dello scrivente, risultano

sufficienti ed adeguate ad evitare rischi elevati per gli interessati.

Considerato, inoltre, che la valutazione d'impatto è un processo dinamico e in continua evoluzione, anche in rapporto ad eventuali modifiche normative e/o organizzative che potrebbero impattare sul trattamento in esame, si suggerisce di sottoporre la DPIA Madre ad una revisione periodica con cadenza annuale.

Si evidenzia quindi al titolare di procedere al riesame della valutazione d'impatto entro un anno dal rilascio del presente parere, così da sottoporla a nuovo parere dello scrivente e se ne consiglia la pubblicazione per estratto sul sito web istituzionale aziendale.

Bologna, li 23 maggio 2024

I Responsabili della Protezione dei Dati

Juri Monducci

Manuel Ottaviano

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

DPIA (Data Protection Impact Assessment)

Trattamento in esame: Ricerca e sperimentazione clinica[1]

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 multisciplinare "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	IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi
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

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 ricomprende, 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). È il principale testo normativo europeo in materia di protezione dei dati personali
Anonimizzazione	È 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

PREMESSA

Presso l'IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi 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'IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi 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 27/02/2024, è stata adottata la presente DPIA avente ad oggetto tutta l'attività di Ricerca scientifica e sperimentazione clinica dell'IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi 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'IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi.

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 del 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'IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi 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' IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi. 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 all´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.

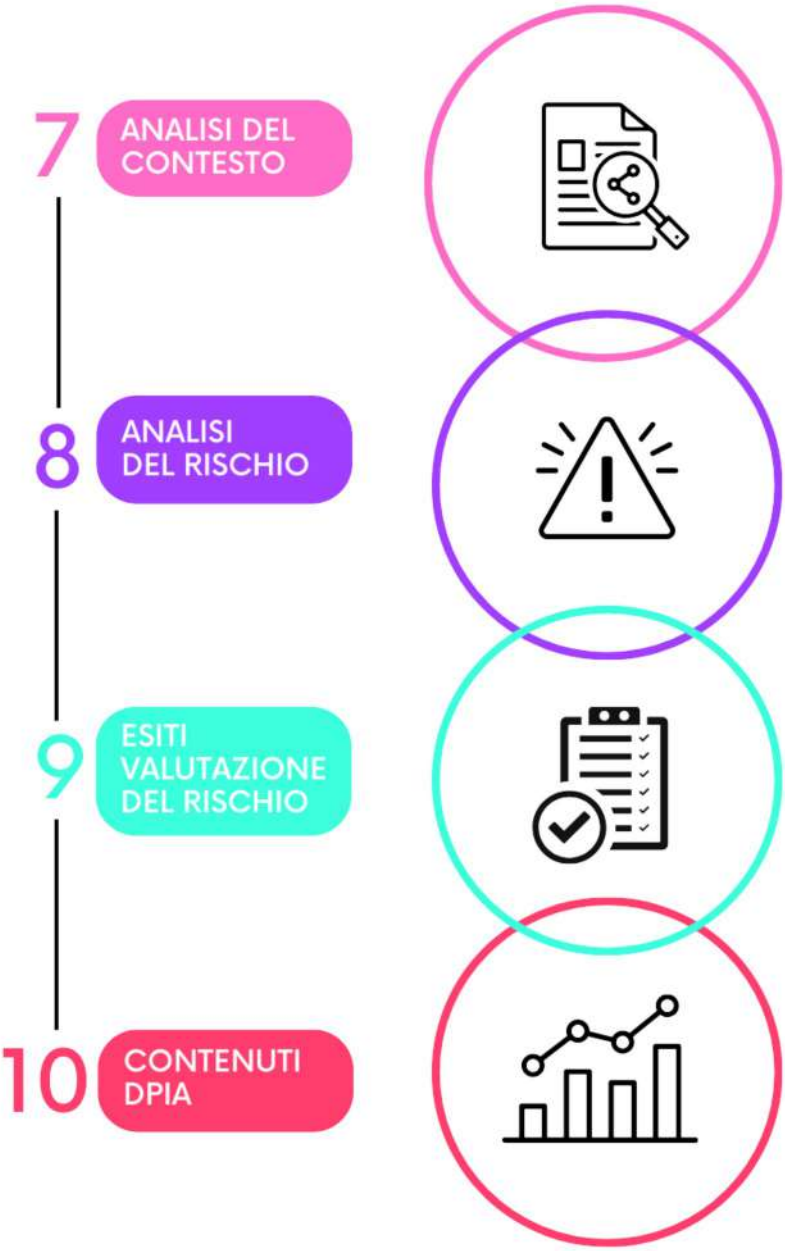
In materia di trasparenza, l'attività di Ricerca si conforma alle indicazioni del Consiglio di Stato (Sez. VI), il quale nella pronuncia del 13 dicembre 2019 n. 8472 ha dichiarato che "dal diritto sovranazionale emergono tre principi, da tenere in debita considerazione nell'esame e nell'utilizzo degli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

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?

Per le attività di Ricerca e di sperimentazione clinica: PI e soggetti dell'equipe di Ricerca o compresi nel Delegation Log.

Per le attività di manutenzione dei sistemi informativi: servizio ICT ed eventuali fornitori.

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

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 autorizzati al trattamento dei dati ex art. 29 GDPR.

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

Il trasferimento di documenti contenenti dati raccolti all'interno degli Studi, può avvenire attraverso l'uso della posta elettronica (preferibilmente attraverso l'utilizzo dello strumento PEC - Posta Elettronica

Certificata - specie se previsto dalle attuali disposizioni Aziendali in materia di comunicazione dei dati) allegando i documenti de quo in formato criptato e inviando con una seconda mail o con altro strumento di comunicazione la chiave di decriptazione.

Inoltre, la comunicazione e il trasferimento potranno avvenire attraverso altri strumenti di sicurezza in uso presso l'IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi (es. condivisione tramite drive proprietario) o secondo la logica Cloud.

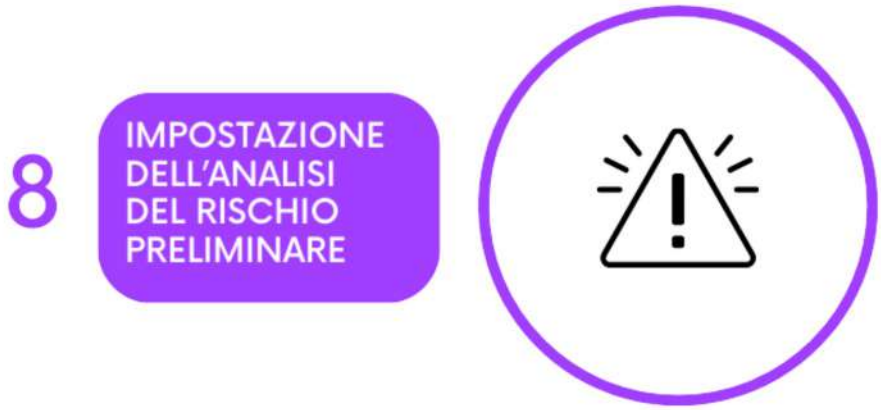
Attraverso i processi di autenticazione e autorizzazione, i destinatari dei dati potranno accedere alle piattaforme condivise per l'estrazione del dataset.

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?

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, nell'informativa per il trattamento dati personali e nel DCSP.

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:

- applicativi Aziendali o individuati dal gruppo di progetto, anche esposti sul web (app sanitarie);
- dispositivi (medici o wearable) Aziendali o individuati dal gruppo di progetto;
- applicativi di machine learning Aziendali o individuati dal gruppo di progetto.

A titolo di esempio si segnala che i dati raccolti su eCRF, in ossequio al principio di minimizzazione, sono esclusivamente quelli definiti nel protocollo della Ricerca e sono resi in forma pseudonimizzata ed inseriti nella piattaforma REDCap o in altre piattaforme messe a disposizione dai Partner di progetto.

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?

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

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?

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, allo stato attuale Andorra, Argentina, Australia (Passenger Name Record), Canada, Isole FaerOer, Giappone, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, USA 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 (CCS 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) il trasferimento deve avvenire sulla base di norme vincolanti di impresa che devono essere approvate dall'autorità competente (in Italia, l'Autorità 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 Data Privacy Framework (DPF), che consente una tutela adeguata degli interessati nei trasferimenti di dati personali tra Europa e Stati Uniti d'America.

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 fattore 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.

	Descrizione del rischio	**Valutazione preliminare di esposizione**
Rischio 1	Distruzione	Basso
Rischio 2	Perdita	Basso
Rischio 3	Distribuzione non autorizzata	Medio
Rischio 4	Accesso ai dati non autorizzato	Medio
Rischio 5	Trattamento non autorizzato	Medio
Rischio 6	Trattamento non conforme alla finalità della raccolta o illecito	Medio

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

In relazione alle misure di sicurezza infrastrutturali ed organizzative di seguito si elencano le seguenti:

Pseudonimizzazione

A ciascun soggetto arruolato nella Ricerca, di norma, viene assegnato un ID alfa-numerico/numerico. La corrispondenza tra tale ID e l'identificativo univoco ospedaliero del paziente è conservata all'interno di uno schema separato. Tale schema è gestito nel Delegation Log della Ricerca da personale individuato e autorizzato dal Titolare.

Crittografia delle password

Le password degli utenti vengono memorizzate in formato criptato, ovvero utilizzando algoritmi e altre tecniche per avere un'elevata resistenza agli attacchi, anche di forza bruta e a dizionario.

Crittografia dei dati in transito

Così come già descritto al punto 7.1.3, qualora sia necessario procedere alla comunicazione o trasferimento dei dati, essi vengono crittografati durante la trasmissione tra le diverse componenti del sistema, anche quando i dati vengono inviati da una applicazione web a un server. L'utilizzo di protocolli di crittografia come HTTPS (TLS > 1.2) per le comunicazioni web è essenziale per proteggere i dati durante il transito.

Controllo degli accessi logici

La sicurezza degli accessi nella componente server è assicurata attraverso privilegi di accesso relativi alle singole funzioni erogabili dal sistema rispetto ad ogni dataset in esso contenuto, ovvero vengono collegati a specifici ruoli coerentemente con il Delegation Log. Inoltre, l'autenticazione può essere gestita utilizzando l'interfaccia LDAP oppure può essere configurata con una two-factor authentication.

Tracciabilità

La tracciabilità dei dati viene garantita attraverso diversi meccanismi:

- L'utilizzo di log per registrare le operazioni effettuate sul database da parte degli utenti o dei processi autorizzati.
- L'utilizzo di tabelle di log per registrare la data e l'ora di creazione, modifica o cancellazione dei record del database.
- L'utilizzo di controlli di qualità per valutare la completezza, l'accuratezza, la consistenza e la validità dei dati.

Archiviazione

I tempi di archiviazione dei dati sono, di norma, definiti nel protocollo di Ricerca o dal massimario di scarto qualora si preveda l'archiviazione di tali dati in forma anonima.

Controllo degli accessi fisici

L'accesso fisico ai locali che ospitano i server, viene regolato dal responsabile ICT, attraverso misure che possono prevedere a seconda dei casi: accesso con badge, area video sorvegliata, ecc.

La tenuta di eventuali dati su supporto cartaceo avviene in armadi chiusi a chiave, con accesso limitato al solo personale autorizzato.

Minimizzazione dei dati

In ossequio al principio di minimizzazione vengono trattati esclusivamente i dati indicati nel dataset necessari per le finalità, degli obiettivi della Ricerca, attraverso la CRF e/o eCRF.

L'accesso all'identificativo univoco ospedaliero del paziente, memorizzato come descritto alla sezione "pseudonimizzazione", è permesso solo ove strettamente necessario ad un numero limitato di soggetti, coerentemente con il Delegation Log.

Vulnerabilità

Viene assicurata la protezione relativamente alle vulnerabilità software attraverso l'attuazione di una manutenzione ordinaria per l'applicazione di eventuali patch di sicurezza.

Inoltre, la protezione relativamente alle possibili vulnerabilità software è garantita attraverso una costante attività di:

- formazione del personale incaricato al trattamento dei dati;
- sviluppo sicuro di procedure di pseudonimizzazione;
- aggiornamento del sistema almeno annuale;
- piani di risposta agli incidenti.

Lotta contro il malware

La misura più importante è tesa ad evitare l'accesso indiscriminato. Inoltre, è previsto il controllo periodico della sicurezza dei server verificando che:

- l'antivirus sia presente, aggiornato e funzionante e che non risultino problemi dalle ultime scansioni;
- non vi sia evidenza di traffico di rete anomalo in uscita, dalla data di ultima verifica.

Backup

Il Titolare è responsabile delle procedure di backup a livello di virtualizzazione o, copia periodica del server. Sono impostati backup giornalieri e retention di almeno 30 gg su server separati.

Manutenzione

La manutenzione del server fisico è demandata al personale del servizio ICT del Titolare.

Sicurezza dei canali informatici

Il Firewall è adeguatamente configurato dal personale del servizio ICT del Titolare.

Sicurezza dell'hardware

Le configurazioni di sicurezza relative all'hardware sono demandate al personale ICT del Titolare.

Protezione contro fonti di rischio non umane

La presenza di backup giornalieri e retention di almeno 30 gg su server separati evita la perdita di dati.

Inoltre vengono effettuati periodicamente controlli per evitare guasti, difetti dell'architettura IT, alimentazione, rischi ambientali.

10.6 Misure organizzative

In relazione alle misure di sicurezza infrastrutturali ed organizzative di seguito si elencano le seguenti:

- Gestione postazioni e dei dispositivi Aziendali
- Designazione del responsabile del trattamento e indicazione delle istruzioni

- Policy in materia di protezione dei dati
- Gestione delle policy in materia di protezione dei dati
- Gestione dei rischi
- Policy per la gestione degli incidenti di sicurezza e le violazioni dei dati personali
- Gestione del personale
- Gestione dei terzi che accedono ai dati
- Vigilanza sul rispetto della prescrizione della normativa sulla protezione dei dati

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.

Procedure: riconoscimento anagrafico e identificazione della persona assistita, ecc.

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

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, 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?	I dati vengono trattati solo da soggetti autorizzati inoltre ogni caso è pseudonimizzato o anonimizzato.
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, 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. L'informativa viene inoltre pubblicata sul sito istituzionale dell'IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi.
6. Il trattamento dei dati comporta l'utilizzo di dati personali già raccolti, che verranno utilizzati per finalità secondarie?	Nei casi di dati appartenenti agli IRCCS si applica l'art. 110 bis IV comma pertanto è consentito il riuso dei dati personali raccolti per finalità di cura. Negli altri casi 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	Al fine di ridurre il rischio per i diritti e le libertà

che le modalità di raccolta dei dati sono adeguate, coerenti e non eccessive, in relazione alle finalità per i quali i dati vengono trattati?	fondamentali degli interessati è prevista la piena applicazione dei principi affermati dall'art. 5 GDPR. Nel dettaglio, i principi individuati dall'art. 5 del GDPR. Dette misure prevedono disposizioni in materia di sicurezza fisica e logica dei sistemi elencati al punto 10.5.
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. Inoltre, sono previste misure organizzative quali ad esempio controlli a campione periodici.
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 agli interessati coinvolti in ragione delle misure di sicurezza adottate.
10. È stato stabilito un periodo massimo di conservazione dei dati?	I dati saranno conservati fino al termine della Ricerca, salvo che gli interessati acconsentano alla conservazione per un periodo più lungo nell'ambito delle finalità del trattamento. 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 – ad eccezione dei casi in cui la raccolta e conservazione avvenga su supporto cartaceo, il dataset in input, a seguito del processo di pseudonimizzazione restituirà in output il dataset pseudonimizzato o anonimizzato, modificato rispetto al dato originale, e il dataset di transcodifica depositato

	su repository Aziendale 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 all'equipe di Ricerca. Normalmente la documentazione cartacea riguarda i dati del progetto (es. Protocollo, parere CE) poiché i dati personali relativi ai soggetti coinvolti vengono trattati prevalentemente in modalità informatizzata. Sicurezza dei canali informatici: tutte le postazioni e i dispositivi dell'IRCCS Azienda Ospedaliero Universitaria S. Orsola-Malpighi 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, disponibili su sito web Aziendale e 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, allo stato attuale Andorra, Argentina, Australia (Passenger Name Record), Canada, Isole FaerOer, Giappone, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, USA 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 (così come definiti al paragrafo 8.6.1), 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

Descrizione del rischio	Rischi inerenti alla protezione dei dati			Opzioni che permettono di evitare o mitigare questo rischio (opzioni/controlli applicati)	Rischi residui		
	Impatto	Probabilità	Rischio		Impatto	Probabilità	Rischio
Distruzione	1	2	BASSO	Backup, monitoraggio, formazione	1	2	BASSO
Perdita	2	2	BASSO	Backup, monitoraggio, formazione	2	2	BASSO
Distribuzione non autorizzata	2	3	MEDIO	Formazione, stratificazione delle autorizzazioni	1	2	BASSO
Accesso ai dati non autorizzato	2	4	MEDIO	Accesso ai dati riservato. Pseudonimizzazione. Gestione postazioni. Controllo degli accessi fisici. Sicurezza dei documenti cartacei. Sicurezza dei canali informatici. Gestione delle politiche di tutela della privacy. Formazione. Stratificazione delle autorizzazioni, PW rinforzata per accedere ai dati (di norma doppia PW), limitazione dei soggetti che hanno	2	2	BASSO

				accesso ai dati,			
Trattamento non autorizzato	2	3	MEDIO	Accesso ai dati riservato. Pseudonimizzazione. Gestione postazioni. Controllo degli accessi fisici. Sicurezza dei documenti cartacei. Sicurezza dei canali informatici. Formazione. Stratificazione delle autorizzazioni,	1	2	BASSO
Trattamento non conforme alla finalità della raccolta o illecito	2	2	BASSO	Accesso ai dati riservato. Pseudonimizzazione. Gestione postazioni. Controllo degli accessi fisici. Sicurezza dei documenti cartacei. Sicurezza dei canali informatici. Formazione. stratificazione delle autorizzazioni,	2	2	BASSO

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

Area	Livelli	Entità di rischio
B	1-4 (rischio accettabile)	bassa (B)
M	5-14 (rischio da ridurre)	media (M)
A	15-25 (rischio da ridurre immediatamente)	alta (A)

APPENDICE C – Piattaforma REDCap

***Scheda sintetica della DPIA condotta sulla piattaforma REDCap* in data 28/01/2022 (PG0003057_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'IRCCS Azienda Ospedaliero Universitaria S.Orsola-Malpighi 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

L'accesso ai dati contenuti nella piattaforma è consentito ai soggetti autorizzati al trattamento ed avviene tramite profilatura e autenticazione strettamente legata alle funzioni svolte.

Il sistema è predisposto per sfruttare diverse tipologie di autenticazione con modalità singola o a doppio fattore nel caso in cui i dati siano esposti su internet.

La gestione delle utenze e degli studi, che avviene attraverso cruscotti ben definiti ad opera del PI o da un suo delegato, permette di stabilire una serie di parametri tra cui: la durata di validità, complessità della password e intervallo di rinnovo della stessa. Le utenze, inoltre, sono agganciate allo specifico progetto e ogni singolo profilo può essere abilitato ad avere accesso a più studi.

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.

L'accesso può essere consentito ad altre strutture, pubbliche o private, a seconda della tipologia di progetto/Ricerca.

Analisi dei rischi

L'assessment effettuato ha preso in considerazione i seguenti rischi:

- Distruzione
- Perdita
- Distribuzione non autorizzata
- Accesso ai dati non autorizzato
- Trattamento non autorizzato
- Trattamento non conforme alla finalità della raccolta o illecito

Per ognuno di essi è stata fatta una attenta e approfondita disamina, anche in rapporto alle peculiarità proprie degli studi e sono state adottate le misure di sicurezza adeguate a mitigare i potenziali rischi per i diritti e le libertà degli interessati.

Per ragioni di sicurezza tali misure rivestono carattere di riservatezza e non sono rese pubbliche.

Conclusione

L'impiego di REDCap, per le esigenze dell'attività di Ricerca riguarderà tutte le strutture dell'IRCCS Azienda Ospedaliero Universitaria S.Orsola-Malpighi, 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 inter Aziendale, 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

Misure sicurezza

Sicurezza Fisica			
SISTEMI ANTINTRUSIONE E ACCESSO FISICO AI LOCALI	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
I locali (edifici, siti, stanze...) dove risiedono uffici, server, data center, archivi etc. sono protetti tramite controlli d'accesso meccanici (cancelli, sbarre, etc.) e/o controlli d'accesso elettronici (badge, codici d'accesso, dati biometrici etc.). I locali sono chiusi a chiave e le chiavi/badge/codici d'accesso sono disponibili solo al personale autorizzato.	**X**		**X**
Le strutture sono protette da allarme, videosorveglianza e guardie.	**X**	Presente servizio GpG nell'area del Policlinico. L'area del Centro Stella (Pad.9) è inserita nelle ronde notturne della Vigilanza aziendale. In programmazione installazione impianto di videosorveglianza e allarme antintrusione al Centro Stella (Pad. 9).	**X**
Al di fuori dell'orario lavorativo, l'accesso ai locali server, ai siti e agli uffici è consentito esclusivamente al personale autorizzato.	**X**		**X**
Visitatori o altre persone esterne/non autorizzate non possono accedere ai locali.	**X**	L'accesso al Centro Stella (Pad.9) è consentito solo mediante badge autorizzati. Eventuale personale esterno/non autorizzato, in caso di necessità di accesso, deve richiedere temporaneamente un badge abilitato previa compilazione di un registro gestito presso ICT.	**X**
SISTEMI ANTINCENDIO	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
E' presente un sistema centralizzato per la rilevazione degli incendi, controllato in modo continuato da un'unità di sorveglianza.	**X**		**X**
Nella sala CED è presente un sistema per la rilevazione degli incendi e un sistema di spegnimento non ad acqua.	**X**		**X**
Sono previsti impianti per l'estinzione degli incendi.	**X**		**X**
Esistono misure di sicurezza idonee alla riduzione degli incendi (es. le porte antincendio vanno tenute chiuse e va predisposto un piano antincendio con dispositivi di spegnimento e uscite di sicurezza)	**X**		**X**
Sono previsti impianti di estinzione incendio automatizzati attivabili in base a condizioni di temperatura locale oppure su comando inviato da sistema di rilevamento.	**X**		**X**
SISTEMI ANTIALLAGAMENTO	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
Esistono misure di sicurezza per la rilevazione tempestiva di perdite d'acqua e un allarme per rilevare la locazione in cui è segnalata la perdita.	**X**	Nel Centro Stella (Pad. 9).	**X**
Sono previsti sistemi antiallagamento (es. pompe) nei piani a livello stradale o interrati.	**X**		**X**
SISTEMI CONTINUITA' DI ALIMENTAZIONE ELETTRICA	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
E' installata un'unità UPS ed un gruppo elettrogeno ed è prevista la possibilità di utilizzare linee separate di continuità.	**X**	Esclusivamente nel Centro Stella (Pad. 9).	**X**
GESTIONE ASSET E PROCESSO DI RICICLO/ RIMPIEGO/ SMALTIMENTO RAEE	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
Tutti gli asset utilizzati per il trattamento di dati personali sono identificati e viene mantenuto, aggiornato e verificato (tramite inventari periodici) un registro di questi asset che specifica owner (responsabile) e utenti dell'asset.	**X**		**X**
Esiste un processo strutturato e formalizzato per l'installazione, l'assegnazione, restituzione e dismissione dei beni (hardware, software) (in particolare: installazione da solo personale autorizzato).	**X**		**X**

Esistenza di un processo che garantisce il rispetto dei seguenti adempimenti: a) nel caso di reimpiego o riciclo dei RAEE, adozione delle misure tecniche per la memorizzazione sicura dei dati quali, a titolo esemplificativo: cifratura file, memorizzazione cifrata dei dati sui dischi rigidi, cancellazione sicura delle informazioni, formattazione a "basso livello" dei dispositivi di tipo hard disk, demagnetizzazione dei dispositivi di memoria magnetici b) nel caso di smaltimento di RAEE: adozione di procedure che garantiscano l'effettiva cancellazione dei dati personali quali: sistemi di punzonatura o deformazione meccanica; distruzione fisica o di disintegrazione; demagnetizzazione ad alta intensità.	**X**		**X**
SICUREZZA DEI DOCUMENTI CARTACEI	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata. I documenti contenenti dati personali non rimangono incustoditi su scrivanie o tavoli di lavoro e non vengono condivisi con personale non autorizzato.	**X**	**IOA29** "ISTRUZIONE OPERATIVA AZIENDALE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI"	
Gli armadi contenenti documenti cartacei sono chiusi con una serratura tradizionale dotata di chiavi individuali	**X**		
I documenti cartacei contenenti dati personali vengono distrutti tramite appositi apparecchi (tritacarte) o comunque in modo tale da non poter leggere/ricostruire i contenuti.	**X**		

Sicurezza Logica dei sistemi informatici e misure relative ai dati personali

CONTROLLO DEGLI ACCESSI	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
L'accesso ai sistemi contenenti dati personali (PC, cartelle condivise, database etc.) avviene tramite codice ID e password, attribuiti a ciascun utente univocamente e individualmente.	**X**		
Gli strumenti di autenticazione (password) sono comunicate agli utenti in modo tale che sia mantenuta la loro riservatezza e non vengono comunicate o usate da altri utenti.	**X**		
Le password sono cambiate periodicamente, è richiesta una lunghezza minima (almeno otto caratteri oppure un numero di caratteri pari al massimo consentito dal sistema) e devono contenere almeno due tipologie diverse di caratteri (ad es. lettere, numeri, caratteri speciali, maiuscoli etc.).	**X**		
Esistono autorizzazioni specifiche per diversi utenti o categorie di utenti, limitando l'accesso ai soli dati strettamente necessari per l'espletamento delle attività. Sono limitati e controllati l'assegnazione e l'uso di diritti di accesso privilegiato.	**X**		
Esiste un processo strutturato e formalizzato che prevede la creazione, modifica e cancellazione degli utenti in caso di inizio, cambio o cessazione del rapporto di lavoro o delle mansioni.	**X**		
Periodicamente avviene la rivisitazione dei diritti di accesso degli utenti e viene verificato periodicamente l'effettivo allineamento tra ID/account attivi e utenti autorizzati.	**X**		
Il sistema centrale è dotato di un SW/sistemi di alert che identifica e registri su log ogni tentativo di effrazione.	**X**	Sugli accessi fisici viene reso disponibile un report periodico. Su quelli logici sono previste alcune misure di contenimento limitate ai principali canali di accesso (mail, vpn, procedure sanitarie).	
CRITTOGRAFIA E PSEUDONIMIZZAZIONE DEI DATI PERSONALI	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**

Sono implementati strumenti di cifratura dei dati statici su supporti di memorizzazione, definendo eventualmente diversi livelli di cifratura/decifratura basato su determinati criteri/regole.	X	Cifratura per i PC portatili; supporti removibili vietati o, se necessari, vengono fornite indicazioni per la cifratura dei dati aziendali ivi memorizzati.	
Sono implementati protocolli crittografici in fase di trasferimento nelle comunicazioni e nelle transazioni (ad es. utilizzo di certificati SSL/TLS).	X		
E' definito e implementato sviluppata e attuata una politica sull'uso, sulla protezione e sulla durata delle chiavi crittografiche attraverso il loro intero ciclo di vita.	X	Una politica più strutturata è disponibile per la gestione dei certificati SSL. Per tutte le altre chiavi crittografiche (interazioni tra i SW) la gestione è demandata ai fornitori.	
Sono implementati tecniche di pseudonimizzazione dei dati.	X		
Sono definite modalità, circostanze e persone autorizzate per risalire all'identità.	X		
PROTEZIONE DELLE RETI	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
Nelle reti sono segregati gruppi di servizi, di utenti e di sistemi informativi; se una parte della rete può essere connessa con terze parti, è prevista la suddivisione in sotto reti.	X		
Il flusso di traffico tra le reti (interne ed esterne) è controllato e sono monitorati gli accessi e i tentativi di accesso; tutti gli utenti di rete sono identificati e autenticati e l'attività dei collegamenti in rete è controllata e registrata centralmente.	X		
L'accesso da remoto è possibile solo in modalità sicura tramite uso di un punto di accesso sicuro e mediante assegnazione di certificati personali con relative chiavi di cifratura.	X		
A seconda del tipo di rete sulla quale il trattamento è effettuato (isolata, privata o Internet), sono implementati sistemi di protezione adeguati: firewall, sonde anti-intrusione o altri dispositivi (attivi o passivi) volti a garantire la sicurezza della rete.	X		
La vulnerabilità delle reti è stata testata tramite penetration test.	X	In particolare attraverrso vulnerability assessment. Per la rete wifi anche con Penetration test.	
CONTINUITA' OPERATIVA	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
Sono effettuate copie di back-up dei dati al fine di garantire la continuità operativa.	X		
Le copie di back-up di tutti i dati sono effettuate su dispositivi rimovibili e sono protetti con meccanismi di protezione dei dati attivi.	X	Solo su server. Non sono in uso strumenti rimovibili.	
E' possibile ripristinare i dati persi dall'ultima copia di back-up.	X		
E' conservata più di una generazione di dati di back-up; tali genererazioni sono trasmesse ad una locazione remota.	X		
Sono presenti server alternativi/sostitutivi per assicurare la continuità elaborativa in caso di eventi imprevedibili.	X		
Sono state testate e vengono regolarmente aggiornate le procedure di Disaster Recovery e Business Continuity Plan per garantire il funzionamento del sistema, anche in caso di guasti tecnici o eventi dannosi.	X	Limitatamente ad alcuni dei sistemi più critici.	X
SICUREZZA OPERATIVA DEI SISTEMI	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
Gli ambienti di sviluppo, test e produzione sono separati per ridurre il rischio di accesso o cambiamenti non autorizzati all’ambiente di produzione.	X		
Il sistema informatico è protetto e costantemente monitorato da programmi in grado di identificare e rimuovere software dannoso (antivirus, antispyware, etc.).	X		
I programmi contro i software dannosi sono costantemente aggiornati.	X		

Non è ammessa l'installazione di software non autorizzato e esistono strumenti per identificare e rimuovere periodicamente software installato dal PC degli utenti.	X		
Gli hardware e software acquistati/sviluppati sono sottoposti a test di vulnerabilità e penetration test.	X	Limitatamente ai principali applicativi aziendali.	
Vengono eseguiti di collaudi formali e test, per assicurare funzionalità, conformità tecnica e requisiti di sicurezza in caso di acquisizione, sviluppo, manutenzione dei sistemi IT, prima di rendere operativi i sistemi.	X		
E' effettuata, mantenuta e riesaminata periodicamente la registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni.	X		
I sistemi per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati.	X		
Le attività degli amministratori e degli operatori di sistema sono sottoposte a log, e questi sono protetti e riesaminati periodicamente.	X		X
MISURE RELATIVE ALLA MINIMIZZAZIONE E ESATEZZA DEI DATI	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
Sono state identificate le categorie dei dati personali da trattare nell'ambito di ciascuna specifica finalità e sono implementate misure che consentono di raccogliere esclusivamente tali dati (ad es. numero limitato di campi, campi predefiniti, limitazione di campi con inserimento di "testo libero", etc.).	X		
I sistemi utilizzati per la raccolta e elaborazione dei dati prevedono controlli automatici finalizzati a contribuire alla completezza e correttezza dei dati (ad es. campi obbligatori, check automatici di coerenza tra dati inseriti, doppio inserimento di dati rilevanti come e-mail, check della lunghezza standard di dati come Codice Fiscale o IBAN, etc.).	X	Limitatamente ai principali applicativi aziendali.	
I dati sono classificati e segregati/strutturati in più parti, a seconda della classificazione, al fine di consentire di trattare solo i dati rilevanti con riferimento ad una determinata finalità, di limitare l'accesso ad altri dati non rilevanti e di ridurre i rischi in caso di accessi non autorizzati.	X		

Misure organizzative

POLITICHE E PROCEDURE DI SICUREZZA	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
Esiste una politica di sicurezza emanata dalla direzione, documentata, accettata e diffusa in tutta l'organizzazione, periodicamente rivista e aggiornata, se necessario.	X		X
Esistono procedure e/o istruzioni operative scritte che prescrivono le regole di sicurezza con riferimento a stampa, archiviazione (incluso i periodi di conservazione), distribuzione, condivisione, trasporto e distruzione dei documenti cartacei che contengono dati personali.	X		
Esistono procedure e/o istruzioni operative scritte che prescrivono le regole relative alla riservatezza e confidenzialità dei dati, le regole di condivisione e comunicazione dei dati (ad es. tramite e-mail), e le regole relativa alla creazione di copie locali/personali di dati.	X		
Esistono policy e regole di comportamento scritte circa il corretto utilizzo dei sistemi informatici (inclusi i mobile devices, accessi da remoto, teleworking, chiavette usb etc.), diffusi a tutti gli utenti e periodicamente aggiornati.	X	**IOA44** "REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE INFORMATICHE, CON PARTICOLARE RIFERIMENTO ALLA SICUREZZA E RISERVATEZZA"	

Esistono procedure scritte volte a garantire la sicurezza della sicurezza fisica e dei sistemi IT, relativamente almeno alle seguenti tematiche: - sicurezza fisica degli edifici, siti, locali - gestione e verifica degli accessi - Procedure di back-up e disaster recovery - Gestione degli asset, hardware e software (assegnazione, dismissione, inventari, manutenzione etc) - Gestione degli incidenti di sicurezza informatica - Gestione delle reti e trasmissione dei dati - Gestione delle changes ai sistemi informatici.	X		X
Le informazioni tecniche relative alla configurazione e alla protezione dei sistemi e della rete sono custodite e sono accessibili solo da parte di personale autorizzato.	X		
Nelle procedure esistenti o tramite procedure ad hoc sono definite le modalità di implementare la protezione dei dati personali "by design".	X		
GESTIONE, FORMAZIONE E SENSIBILIZZAZIONE DEL PERSONALE	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
Il processo di selezione del personale (interno o esterno) da coinvolgere nel trattamento dei dati personali e/o nella gestione dei sistemi informatici e/o nella gestione delle misure di sicurezza prevede verifiche su competenze, qualifiche, precedenti esperienze e eventuali altri elementi rilevanti, al fine di assicurare un adeguato livello di preparazione tecnica e affidabilità della risorsa.	X	Personale interno: corsi di formazione sull'uso degli applicativi informatici e sul GDPR, informative email a tutti, corsi security awareness. Personale esterno: a carico fornitori nominati Responsabili.	
Tutto il personale è informato e istruito sui rischi e sulle misure di sicurezza IT e di protezione dei dati personali attraverso lo svolgimento di incontri o corsi di sensibilizzazione/awareness training.	X		
E' previsto un piano di formazione specifico sulla normativa privacy e sui specifici trattamenti dei dati personali per rendere edotto il personale incaricato al trattamento dei rischi individuati e dei modi per prevenire i danni.	X		
La partecipazione ai corsi di formazione è obbligatoria, i partecipanti vengono registrati, e sono previsti test di apprendimento.	X	La formazione specifica su tali temi non è obbligatoria, ma vengono comunque erogati corsi di security awarenss previsti a tutti i neo-assunti.	
MONITORAGGIO DELLE MISURE DI SICUREZZA E AUDIT	**In capo a Titolare**	**Note**	**In capo a Responsabile Lepida**
Sono previsti flussi di comunicazione (ad es. dall'utente vs. funzione IT/service provider/altre funzioni preposte alla sicurezza dei sistemi IT e dei dati) per segnalare incidenti, data breach, debolezze e difetti di funzionamento delle misure di sicurezza adottate	X		X
Sono implementate modalità di monitoraggio della efficacia e affidabilità delle varie misure di sicurezza tecniche e organizzative e di protezione dei dati e sono pianificate attività di riesame periodico delle misure	X		X
Vengono periodicamente svolte degli audit /verifiche ad hoc, al fine di verificare l'efficacia e il grado di rispetto/implementazione delle misure tecniche e organizzative e di protezione dei dati.	X		X

Note lepida
Note lepida
Note lepida
Note lepida
Note lepida

Per i soli asset hardware.		
Per i soli asset hardware.		

Note lepida

Note lepida
Note lepida

Note lepida
Note lepida
L'aggironamento dei sistemi segue le policy previste per la BC/DR, certificate dai rinnovi ISO27001
Note lepida

Nel perimetro Lepida.
Note lepida

Note lepida

Nel perimetro Lepida.
Note lepida
Note lepida
Processo di certificazione e rinnovo annuale ISO27001.
Processo di certificazione e rinnovo annuale ISO27001.
Processo di certificazione e rinnovo annuale ISO27001.