VALUTAZIONE DI IMPATTO

Redatto:	vedasi sezione team di lavoro

Verificato:	DPO

Approvato:	Direttore Generale e Direttore Scientifico

Versione:	1.0

Firmato da:
STEFANO MANFREDI
Codice fiscale: MNFSFN62D12D150X
Valido da: 15-11-2023 11:12:13 a: 15-11-2026 01:00:00
Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT
Riferimento temporale 'SigningTime': 07-11-2024 16:56:59
Motivo: Approvo il documento

Firmato da:
VITTORIO LUCIANO BELLOTTI
Codice fiscale: BLLVTR57B05D150F
Valido da: 17-10-2022 13:26:12 a: 17-10-2025 01:00:00
Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT
Riferimento temporale 'SigningTime': 07-11-2024 14:44:18
Approvo il documento

DATI DI CONTROLLO DEL DOCUMENTO

Storia del documento				
versione	data	capitolo/paragrafo	modifica apportata	motivo modifica
01	2.08.24	---	Nessuna	Prima versione

Sommario

1. Informazioni generali

1.1 Titolare del trattamento

La presente DPIA è stata redatta dalla Fondazione S. Matteo, in qualità di Titolare del trattamento ("Titolare del trattamento" o "Fondazione").
Tale ruolo è assunto in quanto la Fondazione è il promotore dello studio avendone determinato finalità e mezzi di trattamento.
Il Principal Investigator (Responsabile dello studio) è la dott.ssa Stefania Paolucci

1.2 Contesto di riferimento

Oggetto della presente valutazione d'impatto (Data Protection Impact Assessment – DPIA) è il trattamento dei dati personali dei pazienti che hanno ricevuto prestazioni sanitarie nell'ambito delle attività di cura presso tutti i reparti della Fondazione Policlinico San Matteo di Pavia e ai quali è stata diagnosticata sospetta Malaria/Leishmania/Pneumocistosi, al fine di condurre uno studio multicentrico, retrospettivo, osservazionale, dal titolo "L'introduzione della PCR in microbiologia e parassitologia".

1.3 Standard di riferimento per la predisposizione della DPIA

La presente DPIA è stata realizzata utilizzando come base le informazioni contenute nel software sviluppato dall'Autorità francese per la protezione dei dati (CNIL), in conformità alle indicazioni fornite nelle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" (WP 248 rev. 01 e adottate dall'EDPB il 4 aprile 2017 e modificate il 4 ottobre 2017 – "***Linee Guida***").*
Inoltre, per la valutazione del rischio è stata utilizzata la metodologia dell'*European Union Agency For Network and Information Security* ("**ENISA**") descritta all'interno del documento "*Guidelines for SMEs on the security of personal data processing*" raggiungibile al seguente link https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.

Sono stati, infine, tenuti in considerazione alcuni dei requisiti della norma ISO/IEC 29134 "*Information technology — Security techniques — Guidelines for privacy impact assessment":* in particolare, valutazione necessità DPIA (art. 6.2), composizione del DPIA team (art. 6.3.1), piano di trattamento del rischio residuo e revisione e verifica della DPIA (art. 6.5.3 – 6.5.4).

1.4 Descrizione del quadro normativo e regolatorio, standard e buone prassi

- Regolamento UE 679/2016 [cons. 33-50-52-53-62-65-113-156-157-159-160-161-162-163; artt. 5-9-14-17-21-89];
- D.Lgs. 196/2003 (mod. D.Lgs. 101/2018) [artt. 78-100-105-106-110-110 *bis*]"), come modificato da ultimo dall'art. 1, comma 1, della l. 29 aprile 2024, n. 56. di conversione del D.L. 2 marzo 2024, n. 19;
- Allegato A5 - Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018;
- Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR Versione 2.0 Adottate il 7 luglio 2021;

- Provvedimenti Autorità Garante [provv. GPDP 497/2018 riguardante le aut. gen. 9/2016 e aut. gen. 8/2016];
- Provvedimento del 14 gennaio 2021 - Regione Veneto. Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica;
- Convenzione di Oviedo – "Convenzione per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina: Convenzione sui Diritti dell'Uomo e la biomedicina", del 4 aprile 1997;
- GCP - ICH Harmonised Guideline – "Integrated Addendum to Ich E6(r1): Guideline For Good Clinical Practice", del 9 novembre 2016;
- EDPB – "Documento sulla risposta alla richiesta della Commissione europea di chiarimenti sull'applicazione coerente del GDPR, concentrandosi sulla ricerca sanitaria", adottato il 2 febbraio 2021;
- GPDP – Provvedimento del 9 maggio 2024, "Individuazione delle misure di garanzia ai sensi degli artt. 106, comma 2, lett. d) e 110 del Codice";
- GPDP – "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del D. Lgs. 10 agosto 2018, n. 101 – 19 dicembre 2018", pubblicate sulla G.U. n. 11 del 14 gennaio 2019;
- Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Tecniques, April 2014;
- ISO/IEC 20889:2018 - Privacy enhancing data de-identification terminology and classification of techniques;
- ISO 25237:2017 – Health informatics – Pseudonymization;
- ISO/IEC 27559:2022 - Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework;
- NIST - NISTIR 8053 De-Identification of Personal Information, October 2015;
- DICOM PS3:15 2016 – Annex E;
- NIST SP 800-188 De-Identifying Government Datasets: Techniques and Governance, September 2023;
- ENISA, "Data Pseudonymisation: Advanced Techniques & Use Cases Technical Analysis of Cybersecurity Measures iI Data Protection and Privacy", January 2021;
- ENISA, "Privacy Enhancing Technologies: Evolution and State of the Art", March 2017.

1.5 Procedura per la conduzione della DPIA

La presente DPIA si articola nelle seguenti fasi:

- Fase 0: Determinazione della necessità di condurre la DPIA e costituzione del team DPIA
- Fase 1: Descrizione del trattamento
- Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento
- Fase 3: Calcolo del rischio
- Fase 4: Misure di mitigazione del rischio adottate
- Fase 5: Consultazione degli interessati
- Fase 6: Calcolo del rischio residuo, piano di remediation e parere del DPO
- Fase 7: Eventuale consultazione dell'autorità garante per la protezione dei dati personali
- Fase 8: Monitoraggio e riesame nel tempo della DPIA ed eventuale aggiornamento

2. Fase 0: Determinazione della necessità di condurre la DPIA e costituzione del team DPIA

2.1 Necessità di svolgere la DPIA

Il Titolare del trattamento al fine di garantire che il trattamento dei dati relativi allo stato di salute dei pazienti arruolati nell'ambito dello studio sia svolto in conformità al Regolamento UE 2016/679 si impegna a rispettarne i principi fondamentali.

In particolare, si è provveduto a seguire i principi fondamentali relativi alla valutazione d'impatto sulla protezione dei dati di cui al Regolamento (UE) 2016/679 (di seguito GDPR) così come schematizzati nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" del 4 ottobre 2017 pubblicate dal Gruppo di lavoro Articolo 29 (WP29), e si è riscontrato che i trattamenti presi in considerazione possono presentare rischi elevati.

Il trattamento preso in esame, rispetto a quelli individuati nell'allegato 1 al provvedimento del Garante della protezione dei dati personali n. 467 dell'11 ottobre 2018, "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto", rientra nei:

- Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo) – (rif. 6);
- Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse – (rif. 10);

Preso atto che il sopracitato provvedimento asserisce che la valutazione d'impatto sulla protezione dei dati debba essere effettuata ogniqualvolta ricorra almeno un criterio in quanto è indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati, si è ritenuto opportuno procedere all'esecuzione della valutazione d'impatto.

Team di lavoro
Il presente documento è stato redatto da un team composto da:

- Biologo esperto in biologia molecolare;
- Bioinformatico/Data Manager;
- SIA
- Ufficio privacy;
- DPO (per le impostazioni metodologiche e per il parere sulla DPIA stessa).

Il protocollo di studio è stato sottoposto al competente Comitato Etico Indipendente (CET Lombardia 6) della Fondazione IRCCS Policlinico San Matteo di Pavia che ha rilasciato il suo parere positivo, espresso nella riunione del 25/07/2024, con il verbale n.2024-3.11\41 trasmesso con Prot. 0035951/24 e in seguito ha approvato un emendamento dello stesso nella sessione del 19/07/2024, con il verbale numero 2024-3.11\41 trasmesso con Protocollo 00402081/24.

2.2 Piano delle attività

Al termine della predisposizione della DPIA, il documento verrà sottoposto al parere del DPO.

Il team dovrà recepire almeno parzialmente le osservazioni del DPO, evidenziando eventuali scostamenti, per l'approvazione da parte del Legale Rappresentante.

3. Fase 1: Descrizione del trattamento

3.1.1 Il trattamento oggetto della Valutazione di Impatto

Si tratta di uno studio multicentrico, osservazionale, retrospettivo e cross-sectional. Viene condotto su campioni di sangue periferico prelevati a pazienti giunti all'osservazione dei medici di qualunque unità operativa del nostro nosocomio/ dei centri coinvolti (v. allegato), col sospetto diagnostico di malaria/leishmaniosi/Pneumocistosi. Le Unità Operative generalmente coinvolte in maniera preponderante in questa Fondazione sono il Pronto Soccorso (generale e pediatrico) e il reparto di Malattie Infettive. Tali campioni devono essere giunti in ultima analisi all'osservazione dei microbiologi dell'UOC di Microbiologia e Virologia della nostra Fondazione/ dei centri coinvolti. Tali centri invieranno i campioni, corredati dai relativi dati e meta-dati, come da protocollo di studio (v. allegato).
L'invio dei campioni tra centri sarà regolato da MTA e DTA attualmente in fase di elaborazione. Il corriere sarà DHL, e il trasporto sarà concertato e retribuito da San Matteo. Il flusso sarà il seguente: ogni centro invierà tutti i campioni in suo possesso singolarmente e indipendentemente dagli altri centri in un unico invio al San Matteo. L'invio dei dati invece avverrà sempre e solo tramite sistema Redcap.
Lo studio si propone di raccogliere campioni raccolti nell'arco di un periodo di tempo di circa 10 anni precedentemente all'inizio dello studio.
la raccolta dati verrà eseguita tramite sistema Redcap e verrà organizzata in una tabella che riporterà per ogni campione le informazioni microbiologiche, biochimiche e cliniche relative al paziente al momento del prelievo, omettendo dati anagrafici e date. I pazienti risulteranno così pseudonimizzati.

- Data di inizio prevista: data stimata secondo protocollo: 1 Settembre 2023. Lo studio è iniziato e ha parzialmente raggiunto gli obiettivi preposti per il primo anno e alcuni degli obiettivi preposti per il secondo anno e proseguirà non appena si renderanno di disponibili tutte le autorizzazioni/approvazioni necessarie ed infine la Deliberazione aziendale di autorizzazione alla prosecuzione dello studio
- Durata stimata dello studio osservazionale: 2 anni

L'obiettivo principale dello studio osservazionale no-profit è l'acquisizione di maggiori informazioni cliniche, anamnestiche e prognostiche e conoscenze scientifiche riguardanti malaria, leishmaniosi e pneumocistosi e il trattamento delle stesse.

Gli endpoint considerati sono:

- Endpoint primario
- L'endpoint primario riguarda una stima della sensibilità della Real Time PCR nell'identificare la presenza dei tre analiti in esame (Leishmania spp, Plasmodium spp e Pneumocystis jirovecii), in comparazione con la metodica tradizionale (ricerca microscopica diretta, previa colorazione standard).
-
- Endpoint secondari:
-
- 1) Correlazione tra la carica parassitaria di Leishmania spp, Plasmodium spp. e Pneumocystis jirovecii individuate tramite Real Time PCR e quelle individuate tramite ricerca microscopica diretta (i risultati delle letture al microscopio saranno uniformati facendo riferimento ai risultati forniti dall'Istituto Superiore di Sanità (ISS), laddove applicabile.
-
- 2) Correlazione tra la carica parassitaria di Plasmodium spp. individuata tramite

ricerca microscopica diretta su emoscopia da sangue capillare e quella individuata tramite emoscopia su emocromo.

-
- Endpoint esplorativo
- Prevalenza dei ceppi individuati tramite sequenziamento

Potenziali benefici derivanti dalla sperimentazione allo studio:

Applicazione di un metodo più sensibile e meno operatore-dipendente, fruibile anche da parte di personale non esperto in parassitologia per esempio in urgenza durante turni di guardia; essendo la ricerca di Plasmodium spp., la diagnosi di specie e la parassitemia in caso di falciparum, indagini microbiologiche che rivestono carattere di urgenza. Allo stesso modo l'applicazione di un metodo più sensibile e quantitativo per la ricerca di Leishmania spp. e Pneumocystis jirovecii potrebbero apportare un miglioramento nella diagnosi e nel follow up di questi microorganismi.

Potenziali rischi derivanti dalla sperimentazione allo studio:

Per la natura osservazionale dello studio, non sono previsti rischi addizionali rispetto a quelli già noti in relazione al normale trattamento di questa tipologia di pazienti.

Vi è un rischio aggiuntivo di accesso illegittimo ai dati di ricerca, che saranno protetti come sotto descritto in modo da minimizzare i rischi di trattamento.

3.1.2 Fasi del processo

3.1.2.1 Progettazione (definizione del protocollo)

Nella fase di progettazione è stata individuata una platea di soggetti rispondenti a determinati criteri (**criteri di eligibilità**) e di **un numero di pazienti** che possa dare **significatività statistica allo studio**. Il numero di pazienti è stato individuato in un range di circa 600 Tuttavia, il numero di pazienti potrà subire variazioni in relazione all'andamento dello studio e alla natura dello stesso che comunque verranno notificate al Comitato Etico competente.
Sono stati individuati:

- Le ricerche già effettuate in materia
- Il set di dati da raccogliere
- Le correlazioni ipotizzate tra le diverse variabili

La fase di progettazione si è conclusa con la predisposizione del protocollo dello studio che ha tenuto conto dei seguenti elementi:

- I criteri di eleggibilità
- I numeri di soggetti da coinvolgere: oltre il numero per la significatività statistica si è ipotizzato di aggiungere un margine per la gestione di eventi quali revoca del consenso, opposizione
- La valutazione della possibilità di informare gli interessati ed acquisire il relativo consenso. Si rimanda all'Autorizzazione Generale sulla ricerca scientifica[1] per un'esemplificazione dei suddetti casi:

[1] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972#5 Negli altri casi, quando non è possibile acquisire il consenso degli interessati, i titolari del trattamento devono documentare, nel progetto di ricerca, 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:

- Deceduti
- Non contattabili
- Non in grado di comprendere l'informativa stessa e/o esprimere un valido consenso

- I dati di partenza
- I dati da raccogliere per lo studio (dettaglio della CRF Case Report Form)
- La relativa codifica (IDC, etc.)
- La precisione dei dati da raccogliere
- Le procedure di data quality applicabili
- Il periodo di conservazione dei dati (7 anni) al termine dello studio Il backup del CRF tramite applicativo Redcap è settato a 7 anni.
- L'elenco dei soggetti coinvolti
- L'individuazione degli strumenti di trattamento applicabili nelle diverse fasi
- Le procedure di eventuali scambi dati con altri soggetti
- Le norme che richiedono/su cui si basa la ricerca
- Gli standard applicabili
- I ruoli privacy
- Altri aspetti privacy (informativa, consenso, trasferimenti, rispetto dei principi)

La fase di progettazione ha tenuto conto dei requisiti degli artt. 5 e 25 del GDPR, per il cui dettaglio si rinvia al par. 4 - Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento.

3.1.2.2 Fase di individuazione dei pazienti eleggibili

Tale fase prevede, almeno come primo step, la consultazione delle seguenti basi dati: cartelle cliniche cartacee o online, referti di indagini biochimiche e microbiologiche tramite i corrispettivi applicativi aziendali dedicati.

La consultazione viene condotta dal personale che partecipa alla Sperimentazione, producendo un'estrazione che contenga solamente:

- I dati previsti dalla CRF, possibilmente già con la precisione e la codifica definite nello studio.
- L'insieme dei dati di controllo previsti dalle procedure di data quality.

3.1.2.3 Pseudonimizzazione

Per quanto riguarda le tecniche di pseudonimizzazione utilizzate si rinvia al paragrafo 6.2.

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 dello studio 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 lo studio in termini di alterazione dei relativi risultati; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, 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 lo studio 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 seguenti prescrizioni 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 nello studio:
- deceduti o
- non contattabili.

In ogni caso, si considerano rispettati i criteri fissati dall'Allegato A5[2].

3.1.2.4 Fase di estrazione e copiatura nella CRF

I dati clinici saranno estratti manualmente, a cura di personale esperto e adeguatamente formato e inseriti nella CRF tramite piattaforma RedCap (REDCap 14.0.15 - © 2024 Vanderbilt University, https://projectredcap.org/). Questa piattaforma sarà gestita dalla SSD Biostatistica e Clinical Trial Center del Policlinico San Matteo. I dati clinici saranno estratti manualmente dalle cartelle cliniche informatizzate/cartacee e dagli applicativi aziendali. Nella prima fase i dati anagrafici del paziente verranno inseriti in un file di conversione excel e in un database excel a parte saranno inseriti il codice del paziente e i dati biochimici, microbiologici e clinici previsti dal protocollo. I citati file excel saranno conservati all'interno di un PC aziendale dedicato, sito nel laboratorio di Microbiologia e Virologia della Fondazione nel quale l'accesso è limitato al personale autorizzato. In seguito i dati presenti sul secondo foglio excel (codice del paziente e dati clinici e di laboratorio) verranno trasferiti su eCRF (Redcap) come descritto, e tutti i files inerenti alla gestione dello studio (eccetto il CRF) saranno distrutti.

In ogni caso non possono essere introdotte chiavi che, anche in combinazione tra loro, portino all'identificazione diretta del paziente, anche facendo uso di informazioni tenute logicamente ed organizzativamente separate. Nello specifico, la CRF dovrà avere come chiave quella individuata nello step di pseudonimizzazione.

3.1.2.5 Fase di data quality

Gli obiettivi di questa fase sono:

- L'accuratezza dei dati inseriti nella CRF
- La verifica che non vi è possibilità di single out di pazienti (K anonimato, L Diversity)

Tale fase può comportare eventuali aggregazioni e/o nuove generalizzazioni (da notificare eventualmente al comitato etico) o l'esclusione dallo studio di pazienti eleggibili ma "singoli" (per esempio un paziente molto anziano).

A valle di questa fase, i dati verranno anonimizzati/de-identificati per le finalità di pubblicazione scientifica.

---

[2] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069637

Art. 4. Identificabilità dell´interessato. Agli effetti dell´applicazione delle presenti regole:

a) un interessato si ritiene identificabile quando, con l´impiego di mezzi ragionevoli, è possibile stabilire un´associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati che la identificano;

b) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:

• risorse economiche;

• risorse di tempo;

• archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;

• archivi, anche non nominativi, che forniscano ulteriori informazioni oltre quelle oggetto di comunicazione o diffusione;

• risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati;

• conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;

Art. 5. Criteri per la valutazione del rischio di identificazione 1. Ai fini della comunicazione e diffusione di risultati statistici, la valutazione del rischio di identificazione tiene conto anche dei seguenti criteri:

a) si considerano dati aggregati le combinazioni di modalità alle quali è associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensità data dalla sintesi dei valori assunti da un numero di unità statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia è pari a tre;

b) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;

c) i risultati statistici relativi a sole variabili pubbliche non sono soggette alla regola della soglia;

d) la regola della soglia può non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unità statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;

e) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;

f) si presume adeguatamente tutelata la riservatezza nel caso in cui tutte le unità statistiche di una popolazione presentano la medesima modalità di una variabile.

In REDCap tale funzionalità è implementata nel modulo 'Data Quality'. Questo modulo consente di eseguire regole di qualità sui dati del progetto per verificare la presenza di discrepanze negli stessi. Nell'ambito dello studio oggetto della presente DPIA, verranno eseguite le seguenti regole predefinite dall'applicativo: Blank values, Blank values (required fields only), Field validation errors (incorrect data type), Field validation errors (out of range), Outliers for numerical fields (numbers, integers, sliders, calc fieldsS).
A valle di questa fase, i dati verranno anonimizzati/de-identificati per le finalità di pubblicazione scientifica.
Tuttavia, verrà comunque mantenuta l'associazione con i rispettivi dati anagrafici del paziente, al fine di poter risalire all'origine dei dati per effettuare studi di follow up per i pazienti in cura presso le Unità Operative coinvolte, oppure in caso di risultati scientifici che possano avere un impatto rilevabile per il soggetto stesso, sulla base di decisioni espresse nel consenso informato alla partecipazione allo Studio. L'esigenza potrebbe manifestarsi anche per provare alla comunità scientifica la validità della ricerca (peer review).

3.1.2.6 Fase di correlazione statistica

In questa fase si procede all'analisi statistica e si confermano (o meno) le ipotesi dello studio. Tipicamente sono utilizzate librerie di analisi statistica. Queste devono essere aggiornate e non comportare trasferimenti di dati a soggetti terzi.

Il Data manager/Bioinformatico del centro di sperimentazione si occuperà, su indicazione del Principal Investigator, di eseguire analisi di tipo descrittivo ed inferenziali per la verifica delle ipotesi. Qualora si rilevi in futuro la necessità di coinvolgere altri soggetti esterni, verranno rivalutati gli elementi del trattamento e i relativi ruoli privacy.

3.1.2.7 Fase di preparazione dei dati da pubblicare

Obiettivo di questa fase è la verifica che i dati da pubblicare siano realmente anonimi, con probabilità di re-identificazione estremamente bassa, verificando che non vi è possibilità di single out di pazienti (K anonimato, L Diversity).

3.1.2.8 Fase di anonimizzazione/cancellazione dei dati

Obiettivo di questa fase è assicurare la completa non collegabilità dei dati ai singoli pazienti.
I dati verranno esportati tramite il modulo "Data Export, Reports and Stats" effettuando uno shift casuale sulle date puntuali, di un valore compreso tra 0 e 364, mantenendo intatti gli intervalli di tempo relativi tra le varie date. Questi dati verranno infine pseudo- anonimizzati seguendo i principi riportati nel documento "De-Identifying Government Datasets: Techniques and Governance" (NIST SP 800-188) ed in particolare ad ogni paziente verrà assegnato un ID numerico (con distribuzione uniforme tra -2147483648 e +2147483647, cioè il minimo e il massimo rappresentabile sulla macchina per quel tipo di dato). La corrispondenza tra tale ID e il numero identificativo del paziente nell'Enrollment log verrà memorizzato in forma criptata (tramite algoritmo di crittografia simmetrica, e.g. AES) all'interno di uno file separato conservato sui server del Titolare, accessibile al solo PI dello studio e gestito da personale autorizzato dal Titolare; il file in questione verrà distrutto non appena verranno caricati i dati in CRF.
Stante la natura e la finalità dello studio in oggetto, si ritiene opportuno conservare la tabella di correlazione per un periodo di 7 anni successivi al termine dello studio.
In seguito, si procederà con la cancellazione sicura (fisica) di tutti i supporti (principali e copie di backup) su cui sono conservati i dati anagrafici di correlazione.

3.1.3 Ruoli e responsabilità collegate al trattamento.

I soggetti che possono intervenire oltre il Titolare del trattamento sono:

- Redcap: Fornitore Biomeris S.r.l. Via Adolfo Ferrata, 5 - 27100 Pavia: responsabile del trattamento per la gestione della eCRF

In qualità di titolari autonomi, tutti gli altri centri coinvolti:

1. Arcispedale Santa Maria Nuova, Reggio Emilia
2. Ospedale Papa Giovanni XXIII, Bergamo
3. Ospedale Pediatrico Bambin Gesù, Roma
4. Azienda Sanitaria Universitaria Giuliano Isontina, Trieste
5. ASST Mantova
6. Ospedale Cà Foncello/ AULSS2 Marca Trevigiana
7. ASST Fatebenefratelli/Sacco, Milano
8. ULSS 4 Veneto Orientale/ Presidio ospedaliero di Portogruaro, Venezia
9. Presidio Ospedaliero Santissima Annunziata, Napoli
10. ASST Crema Ospedale Maggiore
11. Azienda Ospedaliera Universitaria Careggi, Firenze
12. Università degli Studi di Sassari in collaborazione con il Policlinico di Sassari
13. Azienda Ospedaliera di Perugia
14. Ospedale Civile Santa Maria degli Angeli, Pordenone
15. Presidio Ospedaliero Madonna delle Grazie ASM Basilicata, Matera
16. AOU delle Marche, Ancona
17. Azienda Ospedaliera Universitaria Policlinico Paolo Giaccone, Palermo
18. Ospedale Maggiore, Lodi
19. Ospedale San Jacopo, Pistoia
20. AOU Maggiore della Carità, Novara
21. Azienda dei Colli di Napoli "PO D. Cotugno"
22. IRCCS AOU Policlinico Sant'Orsola, Bologna
23. ASST Grande Ospedale Metropolitano Niguarda, Milano
24. Fondazione Humanitas, Milano
25. AOU Modena
26. Ospedale Centrale di Bolzano
27. Ospedale Amedeo di Savoia, Torino
28. Fondazione Policlinico Gemelli IRCCS Università Cattolica del Sacro Cuore, Roma
29. AOU Ospedale di Padova

Vi sono altri soggetti (Comitato Etico, AIFA) che possono intervenire nel processo per le verifiche di competenza.

In ogni caso il personale che accede ad archivi contenenti dati personali anche solo indirettamente identificativi è stato autorizzato se subordinato/parasubordinato oppure nominato Responsabile ex art. 28 GDPR negli altri casi.

3.1.3.1.1 Persone fisiche che intervengono nel trattamento

Nel trattamento intervengono:

- **L'investigatore/sperimentatore principale**: **definisce il protocollo**: assume il ruolo di designato/delegato, cioè di autorizzato con ruolo di impostazione e coordinamento

- **Investigatori/Sperimentatori**: coordinati dall'investigatore principale raccolgono i dati
- **Data manager**: figura non sanitaria che raccoglie e sistematizza i dati. Spesso operano tramite contratti di lavoro parasubordinati con l'Università o con l'Azienda sanitaria. Può essere visto come autorizzato, eventualmente con compiti di Amministratore di sistema in quanto abilita i ricercatori all'applicativo di CRF. Dovrebbe avere conoscenze di pseudonimizzazione e di statistica. Supporta la definizione della CRF e applica ai dati sanitari le trasformazioni di anonimizzazione.
- **Statistico**: ha la responsabilità di condurre i test statistici sui dati: può essere considerato un designato. Se i dati sono sufficientemente de identificati (dati anonimi) potrebbe non avere ruoli privacy

3.1.3.2 Correlazione tra i soggetti e le fasi

Fase	Soggetti giuridici	Persone fisiche
3.1.2.1 Progettazione (definizione del protocollo)	Ente Sperimentatore principale (Titolare)	Investigatore Principale
3.1.2.2 Fase di individuazione dei pazienti eleggibili	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Investigatore
3.1.2.3 Pseudonimizzazione	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Data Manager
3.1.2.4 Fase di copiatura nella CRF	Ente che ha raccolto/ricevuto i dati (Titolare),	Investigatore Principale/Data Manager
3.1.2.5 Fase di data quality	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Data Manager
3.1.2.6 Fase di correlazione statistica	Ente che ha raccolto/ricevuto i dati (Titolare)	Statistico
3.1.2.7 Fase di preparazione dei dati da pubblicare	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Data Manager
3.1.2.8 Fase di estrazione dei dati per altri progetti di ricerca	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Data Manager
3.1.2.9 Fase di anominimizzazione/cancellazione dei dati	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Data Manager

3.2 Dati, processi e beni di supporto

3.2.1 Dati trattati

I dati personali relativi ai pazienti arruolati sono definiti nel progetto "IPP" creato tramite applicativo REDCap.

Dati personali del paziente:
Dati anagrafici: Nome Cognome, data di nascita e data dell'esame (saranno raccolti all'interno di un file di conversione che verrà distrutto al termine della compilazione del CRF Redcap, come già specificato sopra).

- Dati relativi alla salute: condizioni cliniche al momento del prelievo
- Campioni biologici: risultati di analisi biochimiche e microbiologiche

Per l'adozione delle necessarie misure di sicurezza si trattano i seguenti dati degli operatori (Investigatori, Data Manager ecc).

- Dati anagrafici (Nome e Cognome)
- Credenziali di accesso
- Fattore di autenticazione (password, token)
- Mail
- Log delle operazioni effettuate (data e ora di esecuzione, tipologia di operazione compiuta)

  I log di windows registrano le operazioni di accesso al sistema da parte degli utenti.

Dato	Interessato	Sistema di provenienza del dato	Forma
Log delle operazioni effettuate			Chiaro

I log di REDCap registrano tutte le operazioni effettuate sulla eCRF e sui dati da parte degli utenti. Tali log posso essere visualizzati tramite il modulo 'Logging' accessibile ai soli amministratori di sistema e utenti con tale 'User Right' abilitato.

- Dati anagrafici
- Dati di contatto;
- Dati contenuti nella CRF;
- Credenziali di accesso
- Fattore di autenticazione (password, numero cellulare, ID token)
- Mail
- Log delle operazioni effettuate

Tutti i dati sono trasmessi tramite canale sicuro HTTPS con TLS almeno 1.2.

3.2.2 Fonti dei dati

I dati dei pazienti utilizzati per le finalità dello studio sono acquisiti da cartella clinica online o cartacea e applicativi informatizzati dedicati aziendali.

3.2.2.1 Flusso dei dati

I dati dei pazienti interni ed esterni alla Fondazione rimarranno esclusivamente all'interno del presente Ente per tutta la durata dello studio.

L'invio dei campioni tra centri sarà regolato da MTA e DTA attualmente in fase di elaborazione. Il corriere sarà DHL, e il trasporto sarà concertato e retribuito da San Matteo. Il flusso sarà il seguente: ogni centro invierà tutti i campioni in suo possesso singolarmente e indipendentemente dagli altri centri in un unico invio al San Matteo. L'invio dei dati invece avverrà sempre e solo tramite sistema Redcap.

I dati saranno inviati dai centri partecipanti alla Fondazione tramite il caricamento su REDCap.
Specificare anche come verranno inviati i campioni

3.2.2.2

Si veda il capitolo 3 - Fase 1: Descrizione del trattamento.

3.2.2.3 Tipo di operazioni

La tipologia delle operazioni effettuate sono:

Operazioni standard: Raccolta, Registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.

Operazioni particolari: nessuna

Comunicazione mediante trasmissione: I dati personali non sono comunicati a soggetti terzi.

Diffusione: I dati potranno essere diffusi in forma aggregata per pubblicazioni scientifiche.

Profilazione: Nell'ambito di tali trattamenti i dati personali non sono oggetto di processi decisionali automatizzati né di profilazione (ovvero una qualsiasi forma di trattamento automatizzato per valutare determinati aspetti personali, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica) su cui si basi una decisione o che produca un effetto giuridico sull'interessato o che incide significativamente sulla sua persona.

3.2.3 Beni di supporto

I beni di supporto possono essere raggruppati in:

- Fonti dei dati:
  - Cartelle cliniche informatizzate/cartacee
  - Documenti di archiviazione del materiale stoccato in laboratorio
  - Applicativi informatizzati aziendali dedicati alla refertazione di indagini biochimiche e microbiologiche.
- Sistema per la gestione della CRF (e-CRF)
  - Fogli di calcolo Excel
  - Applicativo RedCap (REDCap 14.0.15 - © 2024 Vanderbilt University, https://projectredcap.org/).

- Infrastruttura:

- Computer dedicato, fisicamente localizzato presso UOC di Microbiologia e Virologia
- Share di rete su server aziendale ubicati presso i DATACENTER della fondazione
- Firewall: Fortigate (versione 7.4.6) con filtri IPS e protezioni antimalware e WAF
- Bilanciatori hardware: in HA
- Storage: replicati presso i datacenter della fondazione
- Sistema di log management: centralizzato in cloud
- Sistema di monitoraggio: centralizzato in cloud
- Rete: collegamento da Intranet aziendale, e connessione protetta da rete pubblica

4. Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento

4.1 Proporzionalità e necessità

Lo scopo di miglioramento del processo di cura/prevenzione e più in generale della salute della collettività si viene a contrappore al diritto alla riservatezza dei singoli. Il miglioramento è tanto più urgente quanto le patologie hanno effetti socioeconomici importanti. D'altra parte, gli impatti sui pazienti sono tanto maggiori quanto le patologie destano allarme sociale e potenziale discriminazione.

I dati personali sono indispensabili per la qualità della ricerca. Le fasi di verifica dei risultati sono un requisito fondamentale di un processo di qualità. Queste, quindi, richiedono una collegabilità del dato alle informazioni cliniche primarie e di conseguenza all'identità del paziente. La strategia principale per rendere il trattamento il meno impattante possibile sulla riservatezza è la minimizzazione della collegabilità tramite tecniche di minimizzazione e pseudonimizzazione dei dati.

4.1.1 Finalità esplicite e legittime

Le finalità del trattamento sono:

1) Di ricerca scientifica: valutazione di particolari protocolli sanitari, efficacia di protocolli di prevenzione, valutazione degli effetti di comorbilità

4.1.2 Fondamenti legali del trattamento

La base giuridica del trattamento si fonda su:

- Art. 110 bis c.4 codice privacy

4.1.3 I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario al conseguimento delle finalità del trattamento ("Minimizzazione dei dati")

Ogni dato raccolto è direttamente e specificatamente funzionale alle necessità per le quali è stato raccolto ed è pertanto pertinente rispetto alle finalità sopra esplicitate.

4.1.4 Accuratezza ed aggiornamento dei dati

Gli Sperimentatori verificano la correttezza dei dati raccolti sulla scheda raccolta dati confrontandoli con quelli presenti sulla cartella clinica del partecipante. I dati sono raccolti e trattati da un numero ristretto di persone: Principal Investigator e personale del gruppo di ricerca autorizzato.
Si assume che la documentazione clinica di origine (cartella clinica) sia accurata (documento di fede privilegiata).
Le procedure di data quality previste sono tese a verificare queste proprietà del dato.

I dati verranno trattati mediante processo di pseudonimizzazione, ovvero ad ogni soggetto partecipante allo studio verrà assegnato un codice che verrà utilizzato nello studio, come descritto nel paragrafo 6.2. La chiave per risalire all'oggetto sarà conosciuta solo dal Principal Investigator e dai ricercatori del gruppo di ricerca autorizzati dal PI.
I dati raccolti saranno oggetto di un'attività di anonimizzazione, sulla base del WP 216 5/2014 per la pubblicazione e alla fine dello studio.

4.1.5 Durata della conservazione dei dati

I dati in forma direttamente identificabile sono conservati a norma di legge nella documentazione clinica (ambito escluso dalla presente DPIA).

La tabella di conversione contenente i dati anagrafici e direttamente identificativi del paziente verrà distrutta subito dopo l'inserimento dei dati in CRF.
I dati conservati nella CRF saranno conservati in modalità segregata per 7 anni dopo il termine dello studio sotto forma di backup creato dal sistema. La CRF verrà chiusa al termine dello studio, in seguito non saranno più consentiti accesso e modifiche alla CRF stessa con le credenziali fornite ai ricercatori per Redcap.
Tale periodo di conservazione si rende necessario al fine di costruire analisi e studi futuri, volti a migliorare le conoscenze demografiche, cliniche, diagnostiche e terapeutiche e la pratica clinica.

I risultatati dello studio (dati anonimi) verranno conservati a tempo indeterminato.

È fatta salva, come detto in precedenza, la conservazione dei dati personali, anche particolari, per un periodo superiore, nei limiti del termine di prescrizione dei diritti, in relazione ad esigenze connesse all'esercizio del diritto di difesa in caso di controversie.

4.2 Controlli per proteggere i diritti degli interessati

4.2.1 Come sono informati gli interessati circa il trattamento

Gli interessati saranno informati mediante l'informativa ex art. 13 GDPR verrà pubblicata sul sito web istituzionale, con richiamo nella sezione News e in un box dedicato, al fine di fornire adeguata pubblicità del trattamento per tutti i casi di impossibilità di contatto con i singoli interessati (o di altre ragioni per la non acquisizione del consenso), in ossequio alle regole deontologiche sulla ricerca scientifica Allegato A5 Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018.
Si rinvia all'Allegato x per la consultazione delle informative e all'allegato x per la consultazione dell'Avviso sullo Studio.

4.2.2 Esercizio dei diritti da parte degli interessati

Per esercitare i diritti previsti dagli artt. da 15 a 22 del GDPR, l'interessato può rivolgersi al titolare del trattamento, anche per il tramite del DPO. I diritti possono essere esercitati con le modalità indicate nell'informativa.
Inoltre, come precisato nell'informativa, l'interessato può sempre esercitare, qualora ritenga che il trattamento dei Suoi dati personali avvenga in violazione di quanto previsto dal GDPR, il diritto di proporre reclamo all'Autorità di controllo, seguendo le indicazioni pubblicate sul sito della stessa (https://www.garanteprivacy.it/modulistica-e-servizi-online/reclamo) o di ricorrere avanti la competente autorità giudiziaria (artt. 77 e 79 del GDPR).

4.2.2.1 Diritto di accesso

Con riferimento al diritto di accesso, l'interessato può ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e in tal caso ottenere l'accesso agli stessi e alle informazioni riportate in dettaglio all'art. 15 del GDPR (es. finalità, destinatari, periodo di conservazione).

4.2.2.2 Diritto di rettifica

L'interessato, inoltre, ha sempre il diritto di ottenere – senza ingiustificato ritardo e comunque entro un mese - la rettifica dei dati personali inesatti che lo riguardano ovvero l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

4.2.2.3 Diritto di cancellazione

Per il trattamento in oggetto che si fonda sul consenso, l'interessato potrà richiedere la cancellazione dei dati personali nell'ambito del presente studio, ai sensi dell'art. 17 del GDPR.

Per quanto concerne, invece, il trattamento dei personali fondato sull'art. 110 del Codice Privacy, il diritto alla cancellazione dei dati potrà essere esercitato anche per il tramite dei soggetti legittimati ai sensi dell'art. 2-terdecies del Codice Privacy.

4.2.2.4 Diritti di limitazione

L'interessato ha il diritto di chiedere la limitazione del trattamento quando:

a. contesta l'esattezza dei dati personali, chiedendo quindi la rettifica, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b. ritiene che il trattamento sia illecito e chiede che ne sia limitato l'utilizzo;
c. i dati personali sono necessari per l'accertamento, l'esercizio o la difesa di un diritto dell'interessato in sede giudiziaria;
d. si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

4.2.2.5 Diritto di opposizione

L'interessato ha il diritto di opporsi al trattamento per motivi connessi alla sua situazione particolare. Il Titolare dovrà astenersi dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. (art. 21 del GDPR).

4.2.3 Obbligazioni dei responsabili del trattamento

Redcap: Fornitore Biomeris S.r.l. è stato individuato quale responsabile del trattamento *ex* art. 28 del GDPR con apposito atto di nomina.

4.3 Trasferimenti al di fuori dello SEE

Non vengono effettuati trasferimenti al di fuori dello Spazio Economico Europeo.

4.4 Rispetto dei principi di Privacy by Design

4.4.1 Rispetto delle strategie

1. Minimizzare: sono trattati soltanto i dati necessari per raggiungere le finalità
2. Aggregare: sono applicate misure di pseudonimizzazione che prevedono tale strategia

3. Nascondere: il trattamento dei dati personali è limitato soltanto a soggetti autorizzati ed i dati vengono conservati in forma cifrata
4. Informare: all'interessato sono fornite tutte le informazioni pertinenti al trattamento in oggetto (informative ex artt. 13 e 14 GDPR)
5. Controllare: all'interessato è garantito l'esercizio dei diritti previsti dalla normativa (artt. 15-22 GDPR). Si rinvia alla procedura di gestione dei diritti degli interessati.
6. Dimostrare: si rinvia alle policy del Titolare del trattamento

5. Fase 3: Calcolo del livello del rischio

Il livello del rischio viene calcolato moltiplicando il valore dell'Impatto (conseguenze negative per gli Interessati di una determinata minaccia) per la Probabilità che una determinata minaccia si possa verificare.
Pertanto, il livello del rischio è pari:

LIVELLO DEL RISCHIO = IMPATTO X PROBABILITÀ OCCORRENZA DELLA MINACCIA

5.1 Calcolo dell'impatto

Si considerano i seguenti livelli di Impatto:

Tabella 1

LIVELLO DI IMPATTO	VALORE	DESCRIZIONE
BASSO	**1**	Gli individui possono andare incontro a **disagi minori**, che supereranno **senza alcun problema** (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
MEDIO	**2**	Gli individui possono andare incontro a **significativi disagi**, che saranno in grado di superare nonostante **alcune difficoltà** (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
ALTO	**3**	Gli individui possono andare incontro a **conseguenze significative**, che dovrebbero essere in grado di superare anche se con **gravi difficoltà** (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
MOLTO ALTO	**4**	Gli individui possono subire **conseguenze significative**, o addirittura irreversibili, **non superabili** (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Il livello d'Impatto deve essere valutato in relazione alle seguenti variabili:

- perdita di riservatezza dei dati;
- perdita d'integrità dei dati;
- perdita di disponibilità dei dati.

Tabella 2

N.	DOMANDA	VALUTAZIONE
I.1.	Si prega di riflettere sull'impatto che una divulgazione non autorizzata (perdita di riservatezza) dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/*rating* di conseguenza.	O **BASSO (1)** O **MEDIO (2)** **X ALTO (3)** O **MOLTO ALTO (4)**
I.2.	Si prega di riflettere sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo ed esprimere una valutazione/*rating* di conseguenza.	**X BASSO (1)** O **MEDIO (2)** O **ALTO (3)** O **MOLTO ALTO (4)**

I.3.	Si prega di riflettere sull'impatto che una distruzione o perdita non autorizzata (perdita di disponibilità) di dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/ *rating* di conseguenza.	**X BASSO (1)** O **MEDIO (2)** O **ALTO (3)** O **MOLTO ALTO (4)**

Il più alto dei tre livelli (perdita di riservatezza, integrità e disponibilità) deve essere considerato come il risultato finale della valutazione dell'Impatto.

Tabella 3

LIVELLO FINALE DELL'IMPATTO	**alto**

5.2 Calcolo della probabilità di accadimento della minaccia

Si deve ora valutare la Probabilità di accadimento delle minacce correlate al trattamento di dati personali nell'ambito del progetto in base al contesto complessivo del trattamento (esterno o interno). Per semplificare questo processo, sono state definite una serie di domande di valutazione (**Tabella 5**) che mirano a sensibilizzare sull'ambiente di elaborazione dei dati (che è direttamente rilevante per le minacce). In tale prospettiva, le domande sono suddivise in quattro diverse aree di valutazione:

1. risorse tecniche e di rete;
2. processi / procedure relativi all'operazione di trattamento dei dati;
3. parti / persone coinvolte nel trattamento dei dati personali;
4. settore di operatività e scala di trattamento.
5. per ciascuna delle predette aree deve essere valutato il livello di probabilità di occorrenza della minaccia in base alla seguente scala:

Tabella 4

Basso	è improbabile che la minaccia si materializzi	Punteggio 1
Medio	c'è una ragionevole possibilità che la minaccia si materializzi	Punteggio 2
Alto	la minaccia potrebbe materializzarsi	Punteggio 3

Tabella 5

RISORSE DI RETE E TECNICHE		
QUESITO	**ESEMPIO**	**RISPOSTA**
Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio *Denial of Service*, *SQL injection*, attacchi *Man-in-the-Middle*), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.	**SI**
È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.	**NO**

Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate a tale accesso).	**NO**
Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico).	**NO**
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono dopo l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza.	**NO**
PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI		
QUESITO	**ESEMPIO**	**RISPOSTA**
I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema	**NO**
L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.	**NO**
I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema *bug* o virus aggiuntivi.	**NO**
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. rete wifi aperte)	**NO**
Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali In Redcap ogni modifica viene registrata mentre su PC aziendale no.	**SI**
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI		

QUESITO	ESEMPIO	RISPOSTA
Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.	**NO**
Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.	**NO**
Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo	**NO**
Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.	**NO**
Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati.	**NO**
SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO		
QUESITO	**ESEMPIO**	**RISPOSTA**
Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento, questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile	**SI**
La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.	**NO**
Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	*Bug* di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (*cyber* o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.	**NO**
Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).	**SI**
Esistono *best practice* di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza.	**NO**

CRITERI PER CALCOLARE IL LIVELLO DI PROBABILITA' (Tabella 6)		
DOMANDE	**RISPOSTE**	**CRITERIO PER CALCOLO DEL RISCHIO PER SEZIONE**
RISORSE DI RETE E TECNICHE		
Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?	**SI**	La valutazione complessiva di questa sezione sarà: BASSO: se si hanno fino a 2 SI MEDIO: se si hanno 3 SI ALTO: se si hanno 4 o 5 SI
È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	**NO**	
Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	**NO**	
Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	**NO**	
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	**NO**	
PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI		
I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	**NO**	La valutazione complessiva di questa sezione sarà: MEDIO: se si risponde SI alle domande n.3 e n.4, in quanto il livello di rischio per questa sezione non può essere considerato 'basso' quando i comportamenti dei dipendenti possono essere causa di perdita di integrità, riservatezza e disponibilità dei dati
L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	**NO**	
I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	**NO**	
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	**NO**	

Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	**SI**	
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI		
Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	**NO**	La valutazione complessiva di questa sezione sarà: BASSO: se si risponde NO alla domanda n.2, in quanto significa che i dati vengono trattati all'interno dei sistemi del Titolare garantendone così allo stesso il pieno controllo MEDIO: se si risponde SI alla domanda n.2, in quanto il coinvolgimento di un terzo fa sì che ci sia meno controllo sul trattamento dei dati stessi
Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	**NO**	
Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	**NO**	
Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	**NO**	
Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	**NO**	
SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO		
Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	SI	La valutazione complessiva di questa sezione sarà: BASSO: se si risponde NO alla domanda n.4, infatti se il sistema IT utilizzato non elabora quantità elevate di dati, il rischio è da considerarsi contenuto MEDIO: se si risponde SI alla domanda n.4, infatti un volume elevato di dati personali conservati ed elaborati in un sistema IT aumenta il rischio
La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	NO	
Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO	
Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	SI	

Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO	dell'impatto di eventuali incidenti di sicurezza ALTO: se dovessero variare i parametri e dovessero esserci 3 o più sì

Tabella 6

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
RETE E RISORSE TECNICHE	Basso	1
	Medio	2
	Alto	3
PROCESSI / PROCEDURE RELATIVI AL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2
	Alto	3
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2
	Alto	3
SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	Basso	1
	Medio	2
	Alto	3

I punteggi attribuiti alle 4 aree nella **Tabella 6** devono essere sommati per calcolare il valore finale di probabilità di occorrenza della minaccia fissato in base alla **Tabella 7** che segue.

Tabella 7

Somma globale della probabilità di occorrenza di una minaccia	LIVELLO DI PROBABILITÀ DELLE MINACCE
4 - 5	Basso
6 - 8	Medio
9 -12	Alto

Nella valutazione finale del livello di Probabilità si è tenuto conto anche delle seguenti considerazioni in relazione alla:

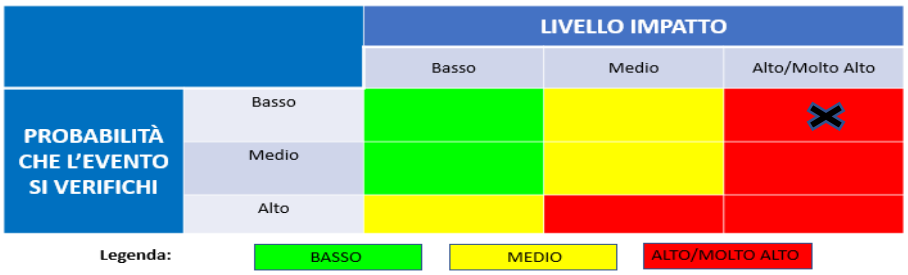
In base alle valutazioni effettuate il livello finale della probabilità di occorrenza delle minacce viene stimato:

Tabella 8

LIVELLO FINALE DELLA PROBABILITÀ DELLE MINACCE	**BASSO**

5.3 Calcolo del livello di rischio

Il livello del rischio sarà dato dalla moltiplicazione del risultato del livello d'Impatto riportato nella **Tabella 3** del paragrafo 5.1 per il risultato del livello di probabilità riportato nella **Tabella 8** del paragrafo 5.2.



LIVELLO DEL RISCHIO	**ALTO**

5.4 Individuazione delle misure che mitigano il rischio

Determinato il livello del rischio, e individuate le minacce e le fonti che potrebbero concretizzarlo, vengono individuate ora le misure di sicurezza che contribuiscono alla mitigazione del rischio stesso.

Perdita di riservatezza

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le principali minacce relative alla perdita di riservatezza riguardano comportamenti umani quali, ad esempio, condivisione dei dati personali con soggetti non autorizzati, errori nelle configurazioni di sicurezza dei sistemi informatici che permettono accessi illegittimi, attacchi informatici esterni, violazione di account.

Quali sono le fonti di rischio?

Le fonti di rischio sono quindi costituite principalmente da operatori interni mal istruiti o insoddisfatti, attacchi esterni tramite phishing, social engineering o sfruttamento di vulnerabilità.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

La probabilità di accadimento delle minacce è mitigata da diverse misure che verranno descritte nel dettaglio nel paragrafo 6. In particolare, le misure che maggiormente contribuisco a garantire una maggior tutela della riservatezza sono la pseudonimizzazione, la prevenzione del malware, la MFA e la segmentazione di rete.

- I dati contenuti nella Base Dati sono infatti pseudonimizzati e non permettono quindi di risalire direttamente all'identità degli Interessati. I dati contenenti la corrispondenza tra i dati anagrafici dei pazienti e il codice identificativo sono infatti salvati separatamente, come indicato nella sezione dedicata al Partizionamento.
- Inoltre, gli accessi ai dati personali da parte degli utenti finali della Piattaforma sono permessi solo a seguito di autenticazione a due fattori (TFA – Two Factor Authentication) attribuendo i permessi sulla base dei ruoli ricoperti.
- Gli accessi fisici sono controllati e le postazioni gestite.
- Viene erogata regolare formazione agli autorizzati al trattamento.

Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, crittografia, gestione del personale, vulnerabilità.

Perdita d'integrità

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le principali minacce relative alla perdita di integrità riguardano ridotti controlli di qualità sulle procedure di data entry. L'errore più probabile potrebbe essere un errore nel mappaggio tra il dato originale e la codifica standard di riferimento. I rischi potrebbero, inoltre, concretizzarsi a seguito di attacchi informatici ed errori umani.

Quali sono le fonti di rischio?

Le fonti di rischio principali riguardano: un operatore interno mal istruito o insoddisfatto, attaccante esterno tramite phishing, social Engineering o sfruttamento di vulnerabilità.

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

Le misure, meglio descritte nel paragrafo 6, adottate per mitigare i rischi di perdita d'integrità sono le seguenti

- Prima di tutto vengono eseguiti diversi controlli di qualità sui dai (descritti alla sezione 3.1.2.5) che ne garantiscono l'integrità: controlli di qualità a campione tramite il modulo 'Data Quality Rules' previsto nella piattaforma REDCap.
- Gli accessi ai dati personali sono permessi solo a seguito di autenticazione a due fattori (TFA – Two Factor Authentication) attribuendo i permessi sulla base dei ruoli ricoperti.
- Gli accessi fisici sono controllati e le postazioni gestite.

Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, crittografia, vulnerabilità.

Perdita di disponibilità

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

La principale minaccia relativa alla perdita di disponibilità riguarda la distruzione accidentale della Base Dati o fisica del server.

Quali sono le fonti di rischio?

Le fonti di rischio per una perdita di disponibilità sono: attività volontaria di un operatore interno con accesso alla Base Dati; attaccante esterno tramite phishing, social Engineering o sfruttamento di vulnerabilità. Errore umano interno per disattenzione/incompetenza. Perdita della password.

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

Le misure adottate per mitigare la perdita di disponibilità dei dati, meglio descritte nel paragrafo 6, riguardano principalmente la presenza di un backup giornaliero mensili ed annuali con retention di almeno 7 gg su server separati gestito a cura del personale IT del Titolare. Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici e degli accessi fisici, archiviazione, partizionamento, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, vulnerabilità, lotta contro il malware, gestione postazioni, gestione dei rischi, gestione del personale, sicurezza dei canali informatici, sicurezza dell'hardware e vigilanza sulla protezione dei dati.

6. Fase 4: Misure di mitigazione adottate

6.1 Crittografia - Cifratura

Vengono implementate le seguenti tecniche di cifratura dei dati personali:

In transito:

- il protocollo di trasporto dei dati tra application server e database è crittografato HTTPS (HyperText Transfer Protocol over Secure Socket Layer) con certificato x509 (Direct Trust mutual Transport-Level Security ovvero mutua autenticazione con scambio di certificat) e protocollo TLS 1.2
- La sequenza dei messaggi di richiesta/risposta avviene dopo aver instaurato il canale di trasmissione sicuro.
- I dati trasferiti durante le attività di backup sono trasmessi su canali sicuri.

At rest:

- I dati della eCRF sono protetti tramite l'utilizzo di una tecnica di autenticazione a due fattori utente e password + codice di verifica (inviato via mail o tramite Google/Microsoft Authenticator) per il database in REDCap.
- Il file relativo alle corrispondenze e la eCRF in REDCap saranno protetti tramite password (con scadenza ogni 60 giorni) differenti con criteri di robustezza quali:
    - Lunghezza minima 9 caratteri
    - Lettere maiuscole e minuscole
    - Cifre di base 10 (da 0 a 9)
    - Caratteri alfanumerici: !@#$%^&*()/_+|~=',-*+:\";?. (esclusi ><\) Il database viene crittografato con algoritmo AES a 128 bit

6.2 Pseudonimizzazione

Vengono implementate tecniche di pseudonimizzazione, al fine di ottenere la separazione tra i dati identificativi del paziente e i dati della eCRF implementata in REDCap.

A ciascun paziente incluso nella eCRF viene assegnato un ID numerico, contestualmente all'ingresso del paziente nello studio tale passaggio è fondamentale per permettere allo Staff dello studio di compilare la eCRF con i dati relativi al paziente corrispondente ed eseguire periodicamente le "Data Quality Rules" (par. 3.1.2.5 Fase di Data Quality) tramite la piattaforma. Lo Sperimentatore Principale e lo Study Coordinator avranno accesso alla corrispondenza tra tale ID e l'identificativo univoco ospedaliero del paziente, che verrà conservato in un file separato (Subject Enrolment Log) conservato in uno storage protetto presso la Fondazione e gestito da personale autorizzato dal Titolare. Non viene, inoltre, riportata la data di nascita del paziente essendo stata sostituita con l'età al momento della procedura. Sono invece presenti date puntuali collegate ai diversi episodi, in quanto ritenute fondamentali per le analisi oggetto dello studio. Tali date potrebbero costituire insieme ad altri identificativi indiretti una potenziale individuazione del paziente solo tramite accesso alla documentazione clinica originaria, salvo una puntuale conoscenza personale del paziente da parte dell'eventuale attaccante che potrebbe comportare l'inferenza di ulteriori informazioni sanitarie. Si ritiene, tuttavia, questo rischio contenuto in quanto in fase di export dei dati verrà applicato uno shift casuale (di un valore compreso tra 0 e 364) alle date puntuali.
La corrispondenza tra nominativo del paziente e il Codice univoco sarà registrata su file Excel separato.

Nello specifico, i dati relativi al paziente saranno:

1. Informazioni relative al record paziente;

Informazioni relative al record diagnosi e situazione clinica del paziente secondo score prognostico di riferimento (https://www.who.int/teams/global-malaria-programme/guideline-development-process/new-and-updated-malaria-guidance) e dati biochimici e microbiologici come da protocollo di studio, che si allega..
Le tabelle saranno collegate per mezzo di un identificativo paziente progressivo univoco (Codice alfanumerico costituito da 6 caratteri es: 6VHNOT).

Il responsabile dei dati e della loro pseudonimizzazione è lo sperimentatore principale.

6.3 Controllo degli accessi logici

Per gli accessi degli "amministratori di sistema" vengono applicate le disposizioni di cui al provvedimento del garante del 2008 e della circolare AGID per le misure di sicurezza della 18/04/2017.
L'accesso alla eCRF tramite l'applicativo REDCap è controllato tramite MFA: password e codice di verifica (inviato via mail o reperibile tramite Google/Microsoft Authenticator).
Il file relativo alle corrispondenze e la eCRF in REDCap saranno protetti tramite password (con scadenza ogni 60 giorni) differenti con criteri di robustezza quali:

- Lunghezza minima 9 caratteri
- Lettere maiuscole e minuscole
- Cifre di base 10 (da 0 a 9)
- Caratteri alfanumerici: !@#$%^&*()/_+|~=',-*+:\";?. (esclusi ><\)

La sicurezza degli accessi nella componente server che permette l'accesso ai dati coinvolge l'autorizzazione che viene gestita sempre all'interno della Piattaforma utilizzando l'interfaccia web REDCap. Viene implementato un modello RBAC (Role-Based Access Control) dove i privilegi, relativi alle singole funzioni erogabili dal sistema rispetto ad ogni dataset in esso contenuto, vengono collegati a specifici ruoli che, in una fase successiva, sono assegnati agli utenti.

Il personale afferente alla SSD Biostatistica e Clinical Trial Center della Fondazione assegna le utenze individuali in REDCap al personale, autorizzato dal Principal Investigator, che si occuperà della creazione della eCRF e dell'inserimento dei dati.

Infrastruttura aziendale:
La sicurezza degli accessi prevede l'identificazione degli utenti tramite le credenziali nominative di dominio e la concessione del pertinente profilo di autorizzazione, determinato sulla base dei privilegi concessi al singolo utente.

Per gli accessi degli "amministratori di sistema" vengono applicate le disposizioni di cui al provvedimento del garante del 2008 e della circolare AGID per le misure di sicurezza della 18/04/2017.
In particolare vengono implementate le seguenti tecniche di autenticazione dei dati personali:

- L'accesso ai dati della CRF è protetto tramite utilizzo di una password per il database Access/Excel.
- Il file relativo alle corrispondenze e il database Access/Excel saranno protetti tramite password differenti con criteri di robustezza quali:
    - Lunghezza minima 14 caratteri

- Lettere maiuscole e minuscole
- Cifre di base 10 (da 0 a 9)
- Caratteri non alfanumerici

6.4 Tracciabilità

La Piattaforma REDCap è dotata di una applicazione interna denominata “Logging”, tramite cui vengono registrate tutte le variazioni al progetto, tra cui Esportazione dei Dati, Variazione ai Campi e alla Struttura della Scheda di Raccolta Dati, Variazione nei Dati, Creazione/Aggiornamento/Cancellazione di Utenti, Creazione/Aggiornamento/Cancellazione di Record, Record Locking & e-signature. Tali informazioni verranno conservate per 7 anni sui server del Titolare.
Infrastruttura aziendale: Vengono tracciati e conservati per un anno i log di eventi di possibile rischio di sicurezza

6.5 Minimizzazione dei dati

La raccolta dei dati si limita a quelli strettamente necessari a perseguire le finalità del trattamento.

- Le fasi di progettazione dello studio ha implicato il rispetto del principio di minimizzazione
- Lo sperimentatore garantisce che i dati previsti nella CRF sono i soli indispensabili alla conduzione dello studio
- L’esperto statistico garantisce che il numero di interessati è il minimo per dare rilievo allo studio

6.6 Lotta contro il malware

La Piattaforma REDCap viene aggiornata all’ultima versione rilasciata stabile e sicura disponibile. Tale aggiornamento è demandato ad un Fornitore esterno.

Le postazioni di lavoro vengono gestite tramite XDR, antivirus continuamente aggiornato e dotate di Firewall (Fortigate, versione 7.4.6 con filtri IPS e protezioni antimalware e WAF).

Il computer sarà su dominio locale e disporrà delle ultime patch di sicurezza nonché antivirus aziendale aggiornato secondo le policy aziendali.

È presente un Next generation firewall (Fortigate versione 7.4.6) con specifiche funzionalità antimalware, filtri IPS e WAF.

- È pianificato specifico audit sulla configurazione dell'apparato.
- Ciascuna postazione di lavoro è dotata di software antivirus, costantemente aggiornato in modo automatico.
- Sono state impartite specifiche disposizioni per verificare puntualmente l'aggiornamento sui sistemi interessati.

In estrema sintesi sono applicati a livello infrastrutturale:

- Strumenti anti "programmi pericolosi" (e.g. antivirus aggiornato periodicamente) in particolare per i client l'antivirus Cynet per i server il prodotto XDR
- Strumenti antintrusione (e.g. impiego di "firewall", segmentazione della rete, ecc.)

Come strumento di Endpoint Detection and Remediation viene utilizzato SPLANK

6.7 Vulnerabilità

Inoltre, la protezione contro le vulnerabilità è garantita attraverso le seguenti attività:

- formazione del personale incaricato al trattamento dei dati
- aggiornamento del sistema almeno annuale
- utilizzo di software e sistemi operativi supportati dal produttore
- sincronizzazione NTP
- piani di risposta agli incidenti
- vapt annuali
- piattaforma di gestione centralizzata delle vulnerabilità

6.8 Backup

Il Titolare è responsabile delle procedure di backup a livello di virtualizzazione o, copia periodica del server database sono impostati backup giornalieri, mensili e annuali e retention di almeno 7 gg su server separati.

6.9 Archiviazione

I dati cartacei sono conservati presso la sede dello studio dello sperimentatore Principale/Promotore.
I dati trattati tramite fogli di calcolo Excel e sistema Redcap sono conservati su un computer dedicato presso l'UOC di Microbiologia e Virologia della nostra Fondazione. Le password per l'accesso al PCR e al CRF verranno custodite presso l'ufficio del Principal investigator in apposito luogo sicuro.
I dati vengono conservati sui server del Titolare fino a 7 anni successivi alla loro raccolta nella eCRF.
Il personale autorizzato della SSD Biostatistica e Clinical Trial Center si occupa della gestione degli accessi e recupero delle password.

6.10 Sicurezza dei documenti cartacei

Non è previsto l'utilizzo di documenti cartacei in merito alla gestione dei dati relativi allo studio

6.11 Sicurezza dell'hardware

Il computer sarà su dominio locale e disporrà delle ultime patch di sicurezza.

Sono applicate le opportune configurazioni di sicurezza relative all'hardware.

6.12 Gestione postazioni

Il Titolare gestisce le proprie postazioni con XDR.
La gestione delle postazioni comprende la postazione di lavoro dedicata, fisicamente localizzata presso l'ambulatorio del direttore della SC Microbiologia e Virologia che viene chiuso a chiave.

Al computer dedicato per le attività avranno accesso solo il Data Manager e il responsabile scientifico del progetto.

Il computer resterà acceso solo durante il suo utilizzo.

Il Titolare ha predisposto un Regolamento per l'utilizzo dei dispositivi informatici, il quale prevede l'applicazione di:

- misure organizzative: istruzioni impartite agli operatori (blocco della postazione, spegnimento ordinato all'uscita, divieto d'installazione di software non autorizzato, etc.)
- misure tecniche: antivirus, aggiornamenti di sistema operativo, etc.

L'accesso da rete pubblica è inibito per il computer utilizzato per la gestione dei dati personali. In ogni caso, l'accesso alla intranet aziendale è protetto da Multi-Factor Authentication (Cisco Duo).

6.13 Manutenzione

La manutenzione del server fisico è demandata al personale IT del Titolare.
Il personale del Fornitore esterno è responsabile del piano di manutenzione ordinaria ed eventualmente evolutiva della Piattaforma REDCap. Il Fornitore esterno esegue un aggiornamento annuale del sistema a versioni compatibili.

6.14 Contratto con il responsabile del trattamento

Il contratto con il responsabile del trattamento contiene opportune istruzioni e disciplina i rispettivi obblighi per assicurare la protezione dei dati personali.

6.15 Controllo degli accessi fisici

Il laboratorio dove è ubicata la postazione fissa è accessibile solo a personale autorizzato. Non è previsto l'accesso da parte dei pazienti ai locali del laboratorio di microbiologia e virologia della nostra fondazione.

Il Titolare ha previsto un protocollo di controllo degli accessi fisici ai locali che ospitano i server, che prevede badge e area videosorvegliata.

6.16 Protezione contro fonti di rischio non umane

Protezione contro fonti di rischio non umane: La presenza di backup giornalieri, mensili ed annuali e retention di almeno 7 gg su server separati evita la perdita di dati.

Eventuali altri controlli legati a guasti, difetti dell'architettura IT, alimentazione, rischi ambientali sono demandati al Titolare.

Il computer utilizzato è comunque collocato in uno stabile diverso rispetto all'ubicazione dei server, in cui la probabilità di allagamento è fortemente limitata.

6.17 Misure di sicurezza in caso di trasferimenti verso Paesi non adeguati

Non sono previsti trasferimenti al di fuori dello Spazio Economico Europeo.

6.18 Politica di tutela della privacy

Le politiche privacy del Titolare del trattamento e dei responsabili del trattamento, relative alla propria organizzazione, sono conformi al GDPR.

Il DPO di Fondazione IRCCS Policlinico San Matteo ha un ruolo di verifica dei trattamenti nei confronti del Titolare del trattamento dati

È stato emesso un Organigramma Privacy che definisce i ruoli all'interno dell'azienda e sono state definite le procedure per la gestione dei diritti degli interessati e la gestione delle violazioni di dati personali.

6.19 Gestione dei rischi

È stata effettuata la valutazione dei rischi i cui risultati sono nello specifico paragrafo.

6.20 Integrare la protezione della privacy nei progetti

La fase di progettazione ha tenuto conto dei requisiti di privacy by design.

6.21 Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Il Titolare ha adottato le seguenti procedure aziendali in materia di trattamento dei dati personali:
- Gestione delle violazioni di dati personali
- Gestione dell'esercizio dei diritti dell'interessato

Gli accordi in essere prevedono la collaborazione di tutti gli Enti coinvolti in caso di incidente.

6.22 Gestione del personale

Il Titolare ha provveduto ad autorizzare il personale a vario titolo coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati).

Inoltre, ha provveduto a comunicare la disponibilità di procedure privacy al personale a vario titolo coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati). Le Procedure sono reperibili sulla intranet aziendale.

Sono state svolte attività di formazione (formazione obbligatoria) per tutto il personale che a vario titolo è coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati). Inoltre pianifica annualmente gli interventi formativi.

6.23 Gestione dei terzi che accedono ai dati

Il CET potrà eventualmente accedere ai dati nello svolgimento dei suoi compiti istituzionali. I dati potranno essere richiesti in via teorica sulla base del L.241/90 da specifici portatori di interesse e con le relative cautele normativamente previste.

6.24 Vigilanza sulla protezione dei dati

Il Titolare ha nominato un DPO con il compito di vigilare sui trattamenti dei dati personali.

7. Fase 5: Consultazione dei rappresentanti e degli interessati

Nello svolgimento della DPIA, il Titolare, valutate le specifiche circostanze del trattamento in esame, ha ritenuto non necessario e sconveniente provvedere alla raccolta delle opinioni dei rappresentanti dei soggetti interessati.

8. Fase 6: Calcolo del rischio residuo, piano di remediation e parere del DPO

8.1 Rischio residuo

Si ritiene che il rischio residuo collegato al trattamento di dati personali per le finalità dello studio in oggetto sia accettabile in quanto sono state adottate misure di sicurezza tecniche e organizzative idonee a contenere il rischio per i diritti e le libertà degli interessati.

8.2 Piano di remediation

Per la minimizzazione del rischio residuo, non sono al momento previste ulteriori misure di sicurezza.

8.3 Opinione del DPO

Il DPO ha espresso un parere in merito al presente documento che è conservato agli atti dell'Ufficio Privacy e DPO.

9. Fase 7: Eventuale consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR

Dato che il trattamento dei dati personali non rientra nei casi previsti dall'art. 110 del D.lgs 196/2003, il Titolare non procederà alla consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR.

10. Fase 8: Monitoraggio e riesame nel tempo della DPIA

Ai sensi del paragrafo 11 dell'art. 35 del GDPR, il Titolare deve:

- verificare che il trattamento dei dati personali sia effettuato conformemente alla DPIA. A tal fine il DPO effettuerà degli audit con cadenza annuale;
- procedere a un riesame del trattamento oggetto di DPIA quando vengono apportate modifiche al trattamento con conseguente variazione del livello di rischio connesso al trattamento stesso, al fine di valutare la necessità di apportare revisioni al DPIA Report ovvero di effettuare una nuova DPIA.

Per valutare se il livello di rischio è variato, si dovrà verificare se sono stati modificati uno o più dei seguenti aspetti:

- Cambiamento sulle attività di trattamento, in termini di:
  - contesto (variazione della localizzazione fisica o di elementi ambientali dell'azienda, nuovi vincoli, funzioni e struttura organizzativa, innesto di politiche e processi aziendali, leggi, norme e contratti);
  - modalità di raccolta dei dati personali (mediante modulo cartaceo o form elettronico, direttamente dall'interessato o indirettamente da terzi)
  - finalità del trattamento;
  - tipologia di dati personali trattati (ad esempio dati genetici);
  - categorie di interessati;
  - soggetti coinvolti nel trattamento (personale interno all'organizzazione o fornitori esterni);
  - combinazioni di dati (integrazione con dati provenienti da altre sorgenti, correlazione di informazioni censite su diverse basi dati);
  - trasferimento di dati all'estero (all'interno della UE o verso paesi od organizzazioni internazionali al di fuori della UE).

- Modifica ai rischi con impatti sui diritti e le libertà delle persone fisiche, derivanti da:
  - Modifica dei sistemi informativi a supporto (subentro di un nuovo Service Provider, migrazione di servizi in Cloud, ecc.);
  - nuovi scenari di rischio (furti di identità e frodi informatiche, introduzioni di attacchi avanzati e azioni non autorizzate)
  - insorgenza di potenziali impatti sulle qualità di riservatezza, integrità e disponibilità dei dati personali;
  - nuove minacce (naturali, ambientali, tecniche, di terrorismo o sabotaggio, provenienti da comportamenti volontari o accidentali);
  - attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali;
  - dismissione di elementi di presidio esistenti.
- Mutamenti nel contesto organizzativo o sociale per l'attività di trattamento, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione.

A seguito delle predette verifiche dovrà essere calcolato il livello di rischio (utilizzando la procedura di cui al punto 7) e acquisito il parere del DPO in merito alla necessità di aggiornare la DPIA ovvero procedere ad una nuova valutazione d'impatto.

In ogni caso, anche a prescindere da modifiche apportate al trattamento, quest'ultimo sarà oggetto di riesame annuale, al fine di verificate se, a seguito di cambiamenti nelle conoscenze tecnico-scientifiche, si sia modificato il livello di rischio e sia quindi necessario adottare misure tecnico organizzative nonché rivedere/integrare la DPIA al fine di mantenere la validità e l'aggiornamento nel tempo della valutazione condotta e dei suoi risultati.

Elenco allegati:

Allegato 1-Foglio Informativo e Consenso trattamento dati _v1.0