ESTRATTO DELLA VALUTAZIONE DI IMPATTO

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.
Gli altri centri partecipanti si qualificano quali Titolari Autonomi.
Il Principal Investigator (Responsabile dello studio) è il Prof. Andrea Anderloni.

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 o che riceveranno prestazioni sanitarie nell'ambito delle attività di cura presso la archivizione della Fondazione IRCCS Policlinico San Matteo e ai quali è stato diagnosticato coledocolitiasi, al fine di condurre uno studio multicentrico, osservazionale, retrospettivo. dal titolo "*Complicanze a lungo termine nei pazienti sottoposti a pregressa dilatazione endoscopica della papilla con pallone: uno studio retrospettivo nazionale*".

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.

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

1.5 Necessità di svolgere la DPIA

Il Titolare del trattamento al fine di garantire che il trattamento dei dati personali 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.

1.6 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.

2. Fase 1: Descrizione del trattamento

2.1.1 Il trattamento oggetto della Valutazione di Impatto

Si tratta di uno studio multicentrico, osservazionale, retrospettivo su pazienti, ai quali è stata diagnosticata una calcolosi della via biliare trattata mediante CPRE e dilatazione endoscopica della papilla e che afferiscono alla S.C. Gastroenterologia ed Endoscopia Digestiva
Lo studio prevede una fase:

1. Fase retrospettiva: progressiva revisione sistematica delle informazioni acquisite a partire dal gennaio 2014 fino a marzo 2023

La raccolta dei dati verrà eseguita tramite piattaforma Redcap (redcap San Matteo).
I dati verranno organizzati utilizzando tabelle, suddivise come di seguito precisato:

1. Informazioni relative agli identificativi corrispondenti al record paziente con eventuali dati di contatto saranno registrati su un form cartaceo denominato "identificativo pazienti studio Wide" che verrà aggiornato manualmente dal personale del centro autorizzato e archiviato presso lo studio della Data Manager in appositi armadi provvisti di chiusura. Si specifica che anche lo studio è provvisto di chiusura con accesso limitato del personale.
2. Informazioni sanitarie relative al record diagnosi e il percorso clinico seguito.

Data di inizio prevista: data stimata secondo protocollo: ottobre 2024. Non essendo stato possibile, lo studio inizierà non appena si renderanno disponibili tutte le autorizzazioni/approvazioni necessarie ed infine la Deliberazione aziendale di autorizzazione allo svolgimento dello studio

- Durata stimata dello studio osservazionale: 12 mesi

L'obiettivo principale dello studio osservazionale no-profit è l'acquisizione di maggiori informazioni cliniche, anamnestiche e prognostiche e conoscenze scientifiche riguardanti l'incidenza di episodi di colangite dopo dilatazione endoscopica della papilla con pallone durante un periodo di follow-up di almeno un anno e il trattamento della stessa nello stesso intervallo di tempo

Gli endpoint considerati sono:

- Incidenza delle colangiti nel tempo

Potenziali benefici derivanti dalla sperimentazione allo studio:

Questo studio non avrà effetti diretti sui partecipanti ma potrà essere utile in futuro ai pazienti con le medesime caratteristiche cliniche al fine di ridurre i rischi di colangite conseguenti alle procedure endoscopiche eseguite.

Potenziali rischi derivanti dalla sperimentazione allo studio:

Per la natura osservazionale dello studio, per la fase retrospettiva, 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.

2.1.2 Fasi del processo

2.1.2.1 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 1.000 (circa 30 soggetti per centro). 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:
    - 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
- L'elenco dei soggetti coinvolti

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:
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.

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

2.1.2.2 Fase di individuazione dei pazienti eleggibili

Tale fase prevede, almeno come primo step, la consultazione delle seguenti basi dati:

revisione delle procedure di colangiopancreatografia retrograda endoscopica (CPRE) per il trattamento della calcolosi della via biliare effettuate nel periodo di tempo indicato nel protocollo, sui portali di refertazione.

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.

2.1.2.3 Pseudonimizzazione

Per quanto riguarda le tecniche di pseudonimizzazione utilizzate si rinvia al paragrafo **Errore. L'origine riferimento non è stata trovata.**.
In ogni caso, si considerano rispettati i criteri fissati dall'Allegato A5[2].

2.1.2.4 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.

---

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 ogni caso non possono essere introdotte chiavi che anche in combinazione tra loro portano 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. Quanto sopra vale per i pazienti arruolati presso gli altri centri, invece, per quanto riguarda i pazienti della Fondazione IRCCS (essendo promotore dello studio), riesce ad accedere alla sezione identificativo di Redcap in cui è possibile risalire all'identità dei pazienti.

2.1.2.5 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.

2.1.2.6 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.

2.1.2.7 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).

2.1.2.8 Fase di estrazione dei dati per altri progetti di ricerca

Fase non prevista.

2.1.2.9 Fase di anonimizzazione/cancellazione dei dati

Obiettivo di questa fase è assicurare la completa non collegabilità dei dati ai singoli pazienti.
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 alla pubblicazione 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.
Inoltre, saranno impiegate le tecniche di de-identificazione indicate nel WP 216 - 5/2014 per i dati personali contenuti nella CRF. Inizialmente, si procederà ad aggregare i dati sostituendo quelli

puntuali con la media su insiemi di pazienti numericamente elevati (oltre i 30) e verranno eliminate tutte le date sostituendole con il solo anno solare.
Verranno inoltre applicati controlli di K-anonimato e L-diversity con valore K=30 e L=15 su tutti dati particolari, eliminando eventuali variabili che non soddisfino il requisito.
Questi controlli verranno eseguiti tramite strumenti software similari ad ARX.
Si procederà in accordo alla ISO/IEC 27559:2022 a verificare periodicamente l'efficacia della procedura di de-identificazione e la robustezza degli algoritmi di crittografia anche tenendo conto delle Linee Guida sulle funzioni crittografiche – Conservazione delle password pubblicate dal Garante e ACN.

2.1.3 Ruoli e responsabilità collegate al trattamento.

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

- Biomeris SRL per le attività di assistenza/manutenzione IT di Redcap: in qualità di Responsabile del trattamento dati;
- I centri satellite (inseriti nell'allegato Wide-lista centri 2): in qualità di titolari autonomi.

Vi sono altri soggetti (Comitato Etico) 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.

2.1.3.1.1 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

2.1.3.2 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

2.2 Dati, processi e beni di supporto

2.2.1 Dati trattati

I dati personali relativi ai pazienti arruolati sono definiti nel documento "protocollo" presentato al Comitato Etico insieme al protocollo di studio e comprendono i dati indicati nella CRF (cfr. Allegato 1).

Dati personali del paziente:

- Dati anagrafici: anno di nascita, età, sesso;
- Dati relativi alla salute: colangite e procedure ad essa relata

2.2.2 Fonti dei dati

I dati dei pazienti utilizzati per le finalità dello studio sono acquisiti da referti elettronici reperibili dai software aziendali: quali cartella elettronica e applicativi in uso per la refertazione delle procedure.

2.2.3 Descrizione del flusso dei dati

2.2.3.1 Flusso dei dati

Si veda il capitolo 2 - Fase 1: Descrizione del trattamento.
I vari centri satellite inseriscono i dati dei propri pazienti sulla piattaforma Redcap di modo da renderli disponibili alla Fondazione IRCCS per l'analisi dei dati.
Fra i dati inseriti non risulta il nome paziente e nemmeno la data di nascita completa, noi potremmo vedere solo l'ID paziente.

2.2.3.2 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.

2.2.4 Beni di supporto

I beni di supporto possono essere raggruppati in:

- Fonti dei dati:
  - Cartelle cliniche
  - Referti elettronici
- Sistema per la gestione della CRF (e-CRF)
  - Applicativo Redcap

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

3.1 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.

3.1.1 Finalità esplicite e legittime

Le finalità del trattamento sono:
Di ricerca scientifica: valutazione di particolari protocolli sanitari, efficacia di protocolli di prevenzione, valutazione degli effetti di comorbilità.
Esse vengono esplicitate nell'informativa.

3.1.2 Fondamenti legali del trattamento

La base giuridica del trattamento si fonda su:
Art. 110 bis. comma 4 Codice privacy.

3.1.3 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.

3.1.4 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 **Errore. L'origine riferimento non è stata trovata.**. 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.

3.1.5 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 CRF è conservata in modalità segregata per 7 anni dopo il termine dello studio.
Tale periodo di conservazione si rende necessario al fine di ottemperare alla regolamentazione in itinere.

3.2 Controlli per proteggere i diritti degli interessati

3.2.1 Come sono informati gli interessati circa il trattamento

È presente un'informativa al trattamento dei dati personali dello studio sul sito della Fondazione IRCCS nella sezione privacy.

3.2.2 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).

3.2.2.1 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).

3.2.2.2 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.

3.2.2.3 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.

3.2.2.4 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.

3.2.2.5 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).

3.2.3 Obbligazioni dei responsabili del trattamento

Biomeris SRL è stato individuato quale responsabile del trattamento *ex* art. 28 del GDPR con apposito atto di nomina.

3.3 Trasferimenti al di fuori dello SEE

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

3.4 Rispetto dei principi di Privacy by Design

3.4.1 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

4. 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

4.1 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 3

LIVELLO FINALE DELL'IMPATTO	ALTO

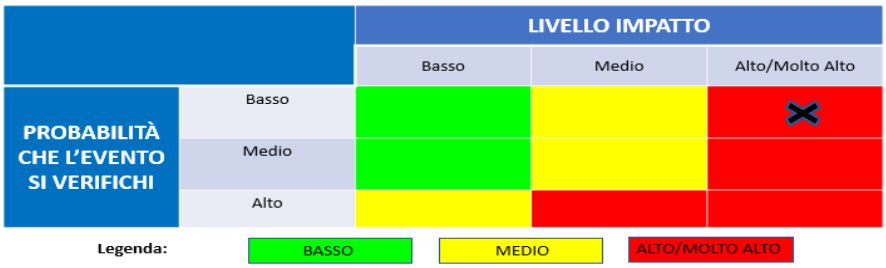
4.2 Calcolo della probabilità di accadimento della minaccia

Tabella 8

LIVELLO FINALE DELLA PROBABILITÀ DELLE MINACCE	**BASSO**

4.3 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 4.1 per il risultato del livello di probabilità riportato nella **Tabella 8** del paragrafo 4.2.



LIVELLO DEL RISCHIO	**ALTO**

.

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

5.1 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.

5.2 Piano di remediation

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

5.3 Opinione del DPO

Il DPO ha espresso un parere al presente documento che è agli atti dell'Ufficio Privacy aziendale.

6. 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.