

MODELLO VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

NB: il modulo si può compilare direttamente su Word.

Le caselle sono spuntabili con il click del mouse.

Le parti da redigere sono anch'esse agevolmente compilabili

**Inserire denominazione del trattamento (es. titolo dello Studio/Progetto)*

REhabilitation Practice and Association with Outcomes in Critically Ill Invasively Ventilated Patients (REPOrt)—an international multicenter observational study

1. Contesto del trattamento oggetto di Valutazione d'Impatto

1.1 Visione d'insieme

Presentazione del trattamento considerato

Descrizione del trattamento (delineare in modo dettagliato il flusso dei dati, dal momento della raccolta a quello della distruzione, indicando anche gli uffici/servizi coinvolti nel trattamento e gli eventuali centri partecipanti in caso di studio multicentrico)	L'obiettivo primario di questo studio osservazionale multicentrico multi-modulare mondiale è descrivere le pratiche riabilitative nelle terapie intensive a livello globale. L'obiettivo secondario è determinare l'associazione degli interventi riabilitativi con i principali risultati delle terapie intensive, come mortalità in terapia intensiva e ospedaliera, durata della degenza, durata della ventilazione invasiva, fallimenti dell'estubazione e mortalità in terapia intensiva e ospedaliera. Esploreremo inoltre le associazioni degli interventi riabilitativi con la qualità della vita e le prestazioni funzionali 28 giorni dopo la dimissione dalla terapia intensiva. Confronteremo anche le pratiche riabilitative e le loro associazioni con i risultati in diverse regioni geoeconomiche. Lo studio è composto da tre moduli, con partecipazione subordinata alle capacità e alla fattibilità locali: (A) un modulo BASICO [obbligatorio per tutti i centri partecipanti], che raccoglie informazioni di base sulle pratiche riabilitative e l'associazione con i risultati. (B) un modulo ESTESO [facoltativo, per i centri interessati], che oltre al modulo BASIC raccoglie dati più granulari sugli interventi riabilitativi, tra cui tipo, tempistica, durata, sicurezza e professionisti che erogano interventi riabilitativi. Questo modulo descrive in dettaglio i seguenti interventi riabilitativi: (1) interventi passivi, come esercizi passivi, stretching, ciclismo, stimolazione elettrica neuromuscolare, ampiezza di movimento continua e passiva; (2) interventi attivi, come terapia fisica, allenamento delle attività quotidiane, mobilizzazione e ciclismo; (3) interventi respiratori come posizionamento, tecniche di pulizia delle vie aeree,
---	--

esercizi di espansione polmonare, dispositivi a pressione positiva delle vie aeree, tecniche di ciclo attivo di respirazione, tecniche di espirazione forzata, manovre di tosse assistita o stimolata, insufflazione-essufflazione e terapia inalatoria; (4) allenamento alla disfagia e test di screening della deglutizione; (5) terapia occupazionale e (6) terapia cognitivo/psicologica.

(C) un modulo di FOLLOW–UP ESTESO [facoltativo, per i centri interessati], che oltre ai risultati di BASE raccoglie la qualità della vita e la prestazione funzionale 28 giorni dopo la dimissione dall'ICU.

Lo studio REPOrt sarà condotto secondo i principi della Dichiarazione di Helsinki e del Medical Research Involving Human Subjects Act (WMO). La gestione dei dati, il monitoraggio e la segnalazione dello studio saranno eseguiti in conformità con le linee guida per la buona pratica clinica (GCP).

L'approvazione per la conduzione di REPOrt in ciascun centro partecipante sarà ottenuta dai comitati etici locali. Poiché questo studio sarà condotto come studio multicentrico, il Principal Investigator (PI) locale di ogni sito partecipante deve ottenere l'approvazione dal Comitato etico di riferimento e necessarie autorizzazioni per condurre questo studio secondo le normative vigenti.

Saranno rispettate le normative nazionali in termini di consenso informato. I dati raccolti saranno disciplinati dal Regolamento generale sulla protezione dei dati (GDPR).

Nella sezione successiva sono descritte, in modo dettagliato, le procedure di acquisizione del consenso e trattamento dei dati.

Acquisizione del Consenso Informato e Trattamento di dati personali

Sebbene il numero e l'ubicazione degli ospedali di reclutamento non siano stati confermati, l'obiettivo è di includere circa 2.400 pazienti, in circa 60 centri in tutto il mondo.

I dati sanitari saranno raccolti dal personale dell'ospedale di reclutamento una volta acquisite le autorizzazioni necessarie a condurre lo studio e il consenso del paziente. Il consenso informato scritto sarà combinato per la partecipazione al modulo BASICO ed ESTESO e separatamente per il modulo FOLLOW–UP ESTESO.

Nel caso in cui il paziente sia temporaneamente incapace e/o incosciente a causa delle condizioni di salute, il consenso sarà richiesto al rappresentante legale, se presente; diversamente si procederà a richiederlo al paziente al ripristino della capacità decisionali. Ove non sia possibile ottenere il consenso del paziente per decesso o per mancato riacquisto della capacità decisionale, al

fine di non compromettere la validità scientifica dello studio, il trattamento dei dati personali sarà effettuato ai sensi dell'art. 110 bis del D.lgs. 196/2003, come modificato dal D.lgs. 101/2018 e s.m.i., e nel Provvedimento n.ro 146 del 5 giugno 2019 nonché successivo Provvedimento del Garante della Privacy del 9 maggio 2024.

I dati raccolti nello studio saranno registrati in un Case Report Form elettronico (eCRF) basato sulla piattaforma software Redcap, gestita dall'IRCCS Azienda Ospedaliera Metropolitana. L'accesso alla piattaforma sarà garantita al PI locale e suoi designati collaboratori solo dopo comprovata acquisizione del parere positivo alla conduzione dello studio da parte del comitato etico di riferimento e necessarie autorizzazioni.

I dati personali identificabili (nome e cognome) saranno raccolti direttamente da un membro del gruppo di ricerca dell'ospedale di reclutamento al momento dell'arruolamento e mantenuti riservati. Gli ospedali di reclutamento saranno responsabili della procedura di pseudonimizzazione dei pazienti e della registrazione sul software RedCap, messo a disposizione dell'Azienda Ospedaliera Metropolitana, dei dati raccolti (opportunamente pseudonimizzati) che non saranno riconducibili ai pazienti dal Promotore e dai suoi collaboratori.

In ciascun centro partecipante, i dati saranno raccolti e inseriti nel database utilizzando un codice identificativo univoco del paziente (pseudonimo), in conformità al Regolamento Generale sulla Protezione dei Dati (GDPR). Il collegamento tra il codice identificativo dello studio e l'identità del paziente sarà conservato esclusivamente presso il centro di arruolamento. I dati identificativi non saranno condivisi tramite eCRF, né con il Promotore né con i suoi collaboratori.

La chiave di ricongiungimento tra il codice di studio e l'identità del paziente sarà conservata esclusivamente presso il centro di arruolamento che ha reclutato il paziente. Il Promotore e i suoi collaboratori non avranno accesso alle chiavi di pseudonimizzazione né disporranno di strumenti che consentano la re-identificazione dei soggetti arruolati. Ciascun centro partecipante sarà responsabile della conservazione della chiave di ricongiungimento in modo sicuro in conformità alla normativa vigente in materia di protezione dei dati personali e alle procedure interne dell'istituzione. La chiave di ricongiungimento sarà conservata per il tempo strettamente necessario al completamento dello studio e agli eventuali obblighi di conservazione previsti dalla normativa applicabile (vedi sezione relativa alla "durata della conservazione prevista").

Non è consentito alcun accesso esterno o condivisione con terze parti dei dati caricati su RedCap.

Tipologia di Dati Raccolti

Le informazioni specifiche dei dati raccolti sono illustrate sotto:
Modulo BASE: per acquisire informazioni di base sulla pratica riabilitativa e di fisioterapia respiratoria in tutto il mondo e outcomes in terapia intensiva e ospedaliera, tra cui:

- o Durata della degenza in terapia intensiva e in ospedale;
- o Durata della ventilazione e dello svezzamento;
- o Gestione delle vie aeree;
- o Complicanze in terapia intensiva e
- o Decesso

Modulo ESTESO: per acquisire dati granulari su tipo, tempistica e durata degli interventi riabilitativi, chi li eroga e valutazione della sicurezza. In questo modulo, ci concentriamo sui seguenti interventi riabilitativi:

- o Interventi passivi (esercizi passivi, stretching, ciclismo, elettrostimolazione muscolare, movimento passivo continuo);
- o Interventi attivi (terapia dell'esercizio, allenamento delle attività quotidiane, mobilizzazione, ciclismo);
- o Fisioterapia respiratoria (posizionamento, tecniche di liberazione delle vie aeree, esercizi di espansione polmonare, dispositivi di pressione positiva finale delle vie aeree, tecniche di ciclo attivo di respirazione, tecniche di espirazione forzata, manovre di tosse assistita o stimolata, insufflazione/essufflazione, terapia inalatoria); e
- o Tecniche aggiuntive (allenamento alla disfagia, test di screening della deglutizione, terapia cognitiva/psicologica).

Modulo FOLLOW-UP ESTESO: per catturare la qualità della vita e le prestazioni funzionali a 28 giorni dalla dimissione dall'ICU. Saranno presi in considerazione i seguenti elementi di valutazione:

- o Epidemiologia, ovvero uso e tecniche di riabilitazione, chi eroga interventi riabilitativi, pratica della ventilazione meccanica, mortalità, durata della degenza in ICU/ospedale, complicazioni/eventi avversi, cure generali in ICU, mortalità;
- o Pratiche riabilitative, ovvero descrizione dettagliata del supporto ventilatorio, fisioterapia, pratica infermieristica, terapia occupazionale, trattamento psicologico e fisioterapia respiratoria; e
- o Outcomes, ovvero mortalità, durata della degenza, durata della ventilazione e qualità della vita e attività fisica dopo la dimissione.

Figura 1. Diagramma di flusso della raccolta dati.

	ICU ADMISSION Patient baseline information and pre-hospital status SAPS II score ICU DISCHARGE Outcome at discharge Patient pronation Ventilator weaning Airway management ICU complications 0 3 7 14 DISC 28 SOFA score Invasive mechanical ventilation setting Non-invasive mechanical ventilation setting Sedation and myorelaxants Temperature Arterial blood gas Delirium and pain assessment Hemodynamic Rehabilitation (general assessment) Level of cooperation using SSQ Muscle strength using MRC Duration of intervention per day Passive interventions (type, duration) Active interventions (type, duration) Respiratory physiotherapy (type, duration) Other techniques Monitoring during intervention Serious adverse events Location at 28-days (home/hospital) Rehabilitation after discharge Return to work and work activity Living with family/alone Swallowing disorder Tracheostomy cannula Home ventilator Clinical frailty scale EQ-5D-5L mRS Mortality BASIC MODULE EXTENDED MODULE EXTENDED FOLLOW-UP MODULE
Finalità del trattamento	Ricerca scientifica in ambito sanitario.
Titolare del trattamento	IRCCS Azienda Ospedaliera Metropolitana (IRCCS AOM)
Data Protection Officer	Nominato
Strutture interne coinvolte (indicando altresì il nome del Direttore di U.O. / Responsabile di S.S.D.)	UO Clinica Anestesiologica e Terapia Intensiva Direttore Prof. Nicolò Patroniti
Eventuali Contitolari del trattamento (compilare solo nel caso in cui sia stato finalizzato uno specifico contratto di contitolarità)	N.A.
Eventuali Responsabili del Trattamento (compilare solo se presente un soggetto esterno all'IRCCS AOM, opportunamente nominato, che svolge attività in nome e per conto dello stesso)	Dipartimento di Scienze della Salute, DISSAL, Università di Genova
Eventuali Sub-Responsabili del trattamento (compilare solo se presente un soggetto esterno che svolge attività in nome e per conto del Responsabile)	N.A.

Eventuali soggetti autorizzati al trattamento (indicati per categorie spuntando le caselle)

- ☒ Dirigenza sanitaria
- ☒ Comparto sanitario
- ☐ Comparto tecnico amministrativo

1.2 Tipologie di dati oggetto di trattamento e categorie di interessati coinvolte

- Selezionare le tipologie di dati trattati:

- ☒ Identificativi
- ☒ Clinici
- ☐ Genetici

- Selezionare le categorie di interessati cui appartengono i dati personali oggetto di trattamento:

- ☐ Dipendenti
- ☐ Consulenti/Collaboratori
- ☐ Utenti/Contraenti
- ☐ Beneficiari o assistiti
- ☒ Pazienti
- ☐ Minori
- ☐ Legali rappresentanti (genitori, amministratori di sostegno, tutori, ecc...)
- ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ Altro (specificare) [Fare clic o toccare qui per immettere il testo.](#)

1.3 Dati, processo e supporti

Descrizione delle tipologie di dati oggetto di trattamento, fonte di provenienza, eventuali destinatari esterni e individuazione dei termini di conservazione

TIPOLOGIA DI DATI	Fonte di Provenienza dei Dati	Eventuali Destinatari (soggetti terzi e non, ex art. 4, c. 1, n. 9)	Termini di Conservazione e Modalità di Archiviazione
-------------------	-------------------------------	---	--

Dati identificativi	E' prevista la raccolta pseudoanonimizzata di dati quali età, genere, razza/ etnia dalla cartella clinica.	N.A.	I dati verranno archiviati sul software REDCap dell'Ospedale Pliclinico San Martino, Genova. I dati verranno archiviati fino al termine dello Studio e Analisi a 48 mesi, successivamente anonimizzati.
Dati clinici	E' prevista la raccolta pseudoanonimizzata di dati clinici dalla cartella clinica. Il processo di pseudoanonimizzazione avverrà in ciascun centro coinvolto e non sarà disponibile per il Promotore o Suoi collaboratori con accesso al REDCap ricondurre il paziente ad un codice identificativo.	N.A.	I dati verranno archiviati sul software REDCap dell'Ospedale Pliclinico San Martino, Genova. I dati verranno archiviati fino al termine dello Studio e Analisi a 48 mesi, successivamente anonimizzati.
Dati genetici	N.A.	N.A.	N.A.

1.4 Altri eventuali soggetti coinvolti nel trattamento

Contitolari del trattamento (art. 26 Reg. UE 2016/679)

Descrizione dell'attività del Contitolare

Denominazione del Contitolare	Attività del Contitolare	Data sottoscrizione accordo di Contitolarità (MODHSMHQA_0002DPO) e riferimento amministrativo (es. numero e data delibera di approvazione/autorizzazione)
N.A.	N.A.	N.A.

Responsabili del trattamento (art. 28 Reg. UE 2016/679)

Descrizione dell'attività delegata al Responsabile

Denominazione del Responsabile	Attività delegate al Responsabile	Data sottoscrizione dell'atto di nomina a Responsabile (MODAZHAG_0004PRIVACY) e riferimento amministrativo (es. numero e data delibera di approvazione/autorizzazione)
Dipartimento di Scienze della Salute, DISSAL, Università di Genova	Project Managment, Data Cleaning, e Analisi Statistica	04.09.2025

Eventuali sub-responsabili del trattamento

Denominazione	Responsabile Principale	Finalità del trattamento affidato	Limiti dell'attività
N.A.	N.A.	N.A.	N.A.

Soggetti delegati/autorizzati al trattamento

Elenco delegati/autorizzati (per categorie)	Sottoscrizione nomina del Delegato del Titolare al trattamento dei dati/nomina a soggetto incaricato/autorizzato secondo i modelli aziendali (SI/NO)
Dirigenza sanitaria	☒ SI ☐ NO
Comparto sanitario	☒ SI ☐ NO
Comparto tecnico amministrativo	☐ SI ☐ NO

2. Studio dei principi fondamentali

2.1 Valutazione delle misure poste a garanzia della proporzionalità e necessità del trattamento

Precisare la finalità perseguita e indicare gli elementi che rendono legittimo perseguirla

Finalità	Legittimità
Ricerca scientifica in ambito sanitario	<i>Descrivere qual è il fine della ricerca, che è resa legittima, con riferimento alle finalità indicate, dal parere favorevole del Comitato Etico competente.</i> L'obiettivo della ricerca è quello di descrivere come avviene la pratica riabilitativa in terapia intensiva a livello globale. Obiettivi secondari sono di determinare l'associazione tra gli interventi di riabilitazione e la mortalità, lunghezza della degenza, durata della ventilazione invasiva, fallimento dell'estubazione, qualità della vita e performance funzionale a 28 giorni dopo la dimissione dalla terapia intensiva

Base giuridica del trattamento (barrare la/le voce/i che interessa/interessano)

1 - Parte prospettica

Per i dati "comuni" (es. anagrafiche, numero di telefono, indirizzo e-mail)

- ☒ l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- ☒ ai sensi dell'art. 110 bis, IV comma, Codice Privacy, il trattamento dei dati originariamente raccolti per attività clinica/assistenziale viene svolto senza il consenso dell'interessato anche per finalità di ricerca in campo medico, biomedico ed epidemiologico, non costituendo questo un trattamento ulteriore così come descritto ai sensi dell'art. 110 bis, I-II-III commi, Codice Privacy, stante la natura di IRCCS dell'Azienda Ospedaliera Metropolitana San Martino

Per le categorie particolari di dati (es. stato di salute, orientamento sessuale, dati genetici, orientamento religioso, ecc.)

- ☒ l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa esprimerlo neppure volendo;
- ☒ ai sensi dell'art. 110 bis, IV comma, Codice Privacy, il trattamento dei dati originariamente raccolti per attività clinica/assistenziale viene svolto senza il consenso dell'interessato anche per finalità di ricerca in campo medico, biomedico ed epidemiologico, non costituendo questo un trattamento ulteriore così come descritto ai sensi dell'art. 110 bis, I-II-III commi, Codice Privacy, stante la natura di IRCCS dell'Azienda Ospedaliera Metropolitana San Martino.

2 - Parte retrospettiva

Per i dati "comuni" (es. anagrafiche, numero di telefono, indirizzo e-mail)

- ☐ l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

- ☐ ai sensi dell'art. 110 bis, IV comma, Codice Privacy, il trattamento dei dati originariamente raccolti per attività clinica/assistenziale viene svolto senza il consenso dell'interessato anche per finalità di ricerca in campo medico, biomedico ed epidemiologico, non costituendo questo un trattamento ulteriore così come descritto ai sensi dell'art. 110 bis, I-II-III commi, Codice Privacy, stante la natura di IRCCS dell'Azienda Ospedaliera Metropolitana San Martino.
- ☐ ai sensi dell'art. 110, I comma 1° periodo, Codice Privacy, ove non sia possibile raccogliere il consenso, il trattamento è svolto a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, in particolare il progetto rientra nei casi previsti dall'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502;
- ☐ ai sensi dell'art. 110, I comma 2° periodo, Codice Privacy, ove non sia possibile raccogliere il consenso, il Titolare del trattamento ha motivato e documentato, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi il Titolare ha adottato misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e sono osservate le garanzie individuate dal Garante a osservare ai sensi dell'articolo 106, comma 2, lettera d), del Codice Privacy (D.Lgs. n. 196/2003 e s.m.i.)

Per le categorie particolari di dati (es. stato di salute, orientamento sessuale, dati genetici, orientamento religioso, ecc.)

- ☐ l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa esprimerlo neppure volendo;
- ☐ ai sensi dell'art. 110 bis, IV comma, Codice Privacy, il trattamento dei dati originariamente raccolti per attività clinica/assistenziale viene svolto senza il consenso dell'interessato anche per finalità di ricerca in campo medico, biomedico ed epidemiologico, non costituendo questo un trattamento ulteriore così come descritto ai sensi dell'art. 110 bis, I-II-III commi, Codice Privacy, stante la natura di IRCCS dell'Azienda Ospedaliera Metropolitana San Martino.
- ☐ ai sensi dell'art. 110, I comma 1° periodo, Codice Privacy, ove non sia possibile raccogliere il consenso, il trattamento è svolto a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, in particolare il progetto rientra nei casi previsti dall'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502;
- ☐ ai sensi dell'art. 110, I comma 2° periodo, Codice Privacy, ove non sia possibile raccogliere il consenso, il Titolare del trattamento ha motivato e documentato, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi il Titolare ha adottato misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma

di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e sono osservate le garanzie individuate dal Garante a osservare ai sensi dell'articolo 106, comma 2, lettera d), del Codice Privacy (D.Lgs. n. 196/2003 e s.m.i.).

Chiarire come si rispetta il principio della “minimizzazione” dei dati trattati (i dati devono essere adeguati, pertinenti, non eccedenti rispetto alle finalità perseguite)

Dettaglio dei dati trattati	Tipologia (C= comuni / S= categorie particolari)	Misure di minimizzazione
Anagrafici	C	La modalità di contatto sarà unica e su indicazione del partecipante espressa al momento della sottoscrizione del consenso informato.
Clinici	S	Si raccolgono esclusivamente i dati previsti nel Case Report Form dello Studio/Progetto
Genetici	S	Si raccolgono esclusivamente i dati previsti nel Case Report Form dello Studio/Progetto

Chiarire come si dimostra che i dati oggetto di trattamento sono sempre esatti e aggiornati

Misure per garantire la qualità dei dati
I dati sono raccolti direttamente presso i pazienti e dalla documentazione clinica raccolta nei Centri che per definizione deve sempre essere esatta in ossequio agli obblighi di tenuta della documentazione sanitaria che incombono alle strutture sanitarie.
Agli interessati è sempre consentito esercitare il diritto di rettifica dei dati di cui all'art. 16 del Regolamento 2016/679/UE
Il PI del centro ha la possibilità di aggiornare le schede ed il trattamento durante il follow-up

Chiarire come si giustifica la durata della conservazione prevista

Tipi dei dati	Durata della conservazione	Motivazione della durata della conservazione (obbligo di legge/scelta del Titolare)	Modalità di conservazione	Modalità di distruzione al termine della conservazione
---------------	----------------------------	---	---------------------------	--

Anagrafici	7 anni, o comunque per tutto il periodo necessario al raggiungimento degli obiettivi dello Studio/ Progetto o comunque per tutto il periodo necessario al raggiungimento degli obiettivi dello Studio/ Progetto	☐ Obbligo di legge ☒ Scelta del titolare	☒ Cartacea ☒ Elettronica	☐ Cancellazione ☒ Anonimizzazione
Clinici	7 anni, o comunque per tutto il periodo necessario al raggiungimento degli obiettivi dello Studio/ Progetto o comunque per tutto il periodo necessario al raggiungimento degli obiettivi dello Studio /Progetto	☐ Obbligo di legge ☒ Scelta del titolare	☒ Cartacea ☒ Elettronica	☐ Cancellazione ☒ Anonimizzazione
Genetici	N.A. o comunque per tutto il periodo necessario al raggiungimento degli obiettivi dello Studio/ Progetto	☐ Obbligo di legge ☐ Scelta del titolare	☐ Cartacea ☐ Elettronica	☐ Cancellazione ☐ Anonimizzazione

2.2 Valutazione delle misure a protezione dei diritti personali degli interessati

Determinazione e descrizione delle misure adottate per fornire l'informativa agli interessati

In particolare, esplicitare le seguenti informazioni:

Misure per garantire il diritto all'informativa	Modalità di somministrazione
Somministrazione di moduli di consenso informato al trattamento dei dati personali	Personalmente dal medico responsabile dello studio o da altro medico da lui delegato

Determinazione e descrizione delle misure per raccogliere il consenso ¹

Misure per la raccolta del consenso	Modalità operative	Giustificazione dell'eventuale impossibilità della loro messa in opera
Da ogni partecipante viene raccolta l'espressione di un apposito consenso informato previa spiegazione dello studio da parte dei medici del Centro o dai loro delegati.	Il modulo di consenso informato è somministrato in forma cartacea cartacea dal medico responsabile dello studio o da medici del Centro da lui delegati.	N.A.

2.3 Determinazione e descrizione delle misure per l'eventuale trasferimento dei dati al di fuori dell'Unione Europea

Tipologia di dati oggetto di trasferimento	Motivazione del trasferimento	Soggetto destinatario	Paese destinatario	Legittimante del trasferimento (decisione di adeguatezza, clausole contrattuali tipo, regole vincolanti di impresa, altre misure di cui all'art. 49 GDPR fra cui consenso, ecc.)
N.A.	N.A.	N.A.	N.A.	N.A.

- Software utilizzato

MI IMPEGNO A UTILIZZARE QUALE SOFTWARE PER IL TRATTAMENTO DEI DATI REDCAP SU RETE DELL'IRCCS AOM.

¹ N.B. Il consenso costituisce una valida base giuridica

Se la base giuridica del trattamento si rinviene nel consenso dell'interessato che deve sempre essere libero, specifico e informato.

Dati trattati dal software e soggetti interessati:

Tipologie dei dati gestiti mediante il prodotto software	SI	NO	N.A.	NOTE
- Il software gestisce tutti i dati indicati al punto 1.2	☐	☒	☐	
- Il software gestisce solo alcuni dati fra quelli indicati al punto 1.2 e nello specifico:	☒	☐	☐	Solo dati clinici, non dati identificativi
Soggetti interessati	SI	NO	N.A.	NOTE
Il software gestisce dati appartenenti a tutti gli interessati indicati al punto 1.2	☒	☐	☐	
- Il software gestisce dati appartenenti solo ad alcuni soggetti indicati al punto 1.2 e nello specifico:	☐	☐	☒	Fare clic o toccare qui per immettere il testo.

- Misure organizzative e tecniche dell'IRCCS AOM

MI IMPEGNO A RISPETTARE LE MISURE TECNICHE E ORGANIZZATIVE ADOTTATE DALL'IRCCS AOM IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

- Conservazione documenti e eventuali campioni biologici

NON PREVISTI CAMPIONI BIOLOGICI

A conferma delle informazioni e delle dichiarazioni inserite nel presente documento.

Genova, 10.03.2026

Il Principal Investigator Dott. Denise Battaglini

(firma) _____



DENISE
BATTAGLINI
Università
degli Studi
di Genova
18.03.2026
10:46:38
GMT+01:00

Il Direttore UO Clinica Anestesiologica e Terapia Intensiva Prof. Nicolò Antonino Patroniti

(firma) _____



NICOLO' ANTONINO
PATRONITI
UNIVERSITÀ DEGLI
STUDI DI GENOVA
18.03.2026 13:45:29
GMT+01:00

2.4 Valutazione delle misure organizzative/giuridiche di protezione degli interessati

Misure a protezione dei diritti degli interessati	Accettabili (A) / migliorabili (M)	Misure correttive previste
Informativa agli interessati	A	
Raccolta del consenso	A	
Individuazione e nomina degli eventuali Contitolari del trattamento identificati e contrattualizzati secondo modello istituzionale	N.A.	
Responsabili: identificati e contrattualizzati	A	
Sub responsabili: identificati e contrattualizzati	N.A.	
Trasferimento extra UE: rispetto degli obblighi in materia di trasferimento dati al di fuori dell'UE	N.A.	

3. Studio dei rischi legati alla sicurezza dei dati

3.1 Valutazione delle misure di sicurezza

Descrizione e valutazione delle misure che contribuiscono a contenere i rischi legati alla sicurezza dei dati (art. 32).

Nel caso di trattamenti svolti per mezzo di uno specifico software

Denominazione software	REDCAP
Fornitore	Installazione locale effettuata da BIOMERIS (sviluppo effettuato ...)
Descrizione sintetica attività gestita	Importazione dati e gestione CRF elettronica
Architettura (web application o client-server)	Web
DBMS	MySQL

Misure di sicurezza circa l'attività di trattamento:

Misure specifiche applicate sui dati trattati	Modalità operative (e giustificazioni se non previste)	Accettabili (A)/migliorabili (M)?	Misure correttive
Cifratura	I sistemi di cifratura utilizzati sono a chiave asimmetrica e tipicamente sono mirati alla gestione criptata dei canali http. È quindi utilizzato il sistema di criptatura SSL/TSL con certificati rilasciati dal CA. Non vengono ad oggi utilizzati sistemi di criptatura dei dati sulle basi dati, pur valutandone l'uso futuro sulle sezioni anagrafiche. I dati sono conservati a livello locale su database separato e protetto	N.A.	
Pseudonimizzazione	Ad ogni paziente viene assegnato un codice la cui chiave è accessibile al solo ricercatore responsabile dello studio e dallo staff da lui delegato	A	
Controllo degli accessi logici	Gli accessi alle applicazioni aziendali avvengono solo a seguito di opportuna profilazione sia per quanto attiene l'autenticazione degli utenti attraverso il sistema Active Directory aziendale utilizzando login e password soggetti a scadenza periodica e criteri di complessità minima, sia per quanto attiene i criteri autorizzativi che sono gestiti direttamente sulle applicazioni ed in particolare sul sistema di gestione autorizzazioni	A	
Tracciabilità degli accessi amministrativi mediante conservazione dei log	È attivo un sistema di log degli accessi amministrativi, che vengono conservati per un periodo di 6 mesi, come da normativa	A	

Controllo di integrità dei dati	Gestione demandata ai fornitori con cui si stipula contratto di assistenza e manutenzione	A	
Procedure di backup dei dati	Mediante un software di gestione dei backup gestito centralmente si procede a eseguire copia dei dati su storage dedicato	A	
Meccanismi di replica dei dati	Per i sistemi considerati critici sono previsti meccanismi di replica presso datacenter secondari	N.A.	
Accesso tramite SPID	Utilizzo di credenziali SPID	N.A.	
Autenticazione a due fattori (MFA)	Utilizzo di doppio fattore di autenticazione (password e codice temporaneo)	N.A.	
Gestione dei profili utente	Per ciascun utente si definisce uno o più profili autorizzativi	A	
Modalità di archiviazione	Su server aziendale protetto	A	

Dati trattati dal software e soggetti interessati:

Tipologie dei dati gestiti mediante il prodotto software	SI	NO	N.A.	NOTE
- Il software gestisce tutti i dati indicati al punto 1.2				Le maschere di raccolta dati sono configurabili quindi la risposta è studio-specifica
- Il software gestisce solo alcuni dati fra quelli indicati al punto 1.2 e nello specifico:				
Soggetti interessati	SI	NO	N.A.	NOTE
Il software gestisce dati appartenenti a tutti gli interessati indicati al punto 1.2				Le maschere di raccolta dati sono configurabili quindi la risposta è studio-specifica
- Il software gestisce dati appartenenti solo ad alcuni soggetti indicati al punto 1.2 e nello specifico:				

Compliance del software:

Rispetto delle misure di sicurezza	SI	NO	N.A.	NOTE
Il software è integrato con sistemi di sicurezza permettendo la conformità al GDPR necessarie per lo scenario d'impiego cui è destinato: Privacy by design; Privacy by default; minimizzazione; pseudonimizzazione.	X			
Oppure: Il software è parzialmente integrato con sistemi di sicurezza. Tuttavia, è possibile sviluppare dei controlli compensativi che permettono la conformità al GDPR necessarie per lo scenario di impiego cui è destinato.				
Il software permette l'autenticazione degli utenti basata su tecniche di <i>strong authentication</i> (autenticazione basata su password ed OTP)		X		
Oppure: Il software permette l'autenticazione degli utenti tramite smart card (CNS, ecc.)				
Sono previste per <i>default</i> tecniche di abilitazione automatica di meccanismi di costruzione di password complesse		X		
Il software tiene traccia (log accessi e log attività) delle operazioni effettuate tramite applicativo, comprese le attività di sola visualizzazione dei dati, per un tempo parametrizzabile.	X			
Il software permette la profilazione degli utenti (dipendenti autorizzati ad istruire le pratiche e quindi al trattamento dei relativi dati personali) in modo granulare da consentire solo la visibilità necessaria al ruolo svolto.	X			
Rispetto delle misure e degli accorgimenti in tema di amministratori di sistema	SI	NO	N.A.	NOTE
È prevista la possibilità di creare livelli differenziati di amministrazione del sistema	X			
È previsto un sistema di registrazione (access log) per gli accessi logici degli amministratori di sistema al database di supporto dell'applicativo	X			
Il sistema di access log ha caratteristiche di inalterabilità, completezza e di verifica della integrità dello stesso	X			
L'access log contiene almeno i riferimenti temporali, la descrizione dell'evento che le ha generate, l'identificazione del soggetto che ha compiuto l'accesso	X			
L'access log è conservato in maniera inalterabile per almeno sei mesi		X		Non alterabile da applicativo, alterabile a livello di database
Misure specifiche per categorie particolari di dati personali o dati personali relativi a condanne penali e reati	SI	NO	N.A.	NOTE
I dati idonei a rivelare lo stato di salute e la vita sessuale/orientamento sessuale sono registrati e conservati separatamente dagli altri dati personali soggetti a trattamenti che non richiedono il loro utilizzo (disaccoppiamento)	X			

Il software consente l'adozione di tecniche di cifratura o di codici identificativi che non esplicitano direttamente il contenuto informativo in relazione alla gestione di dati idonei a rivelare lo stato di salute o la vita sessuale/orientamento sessuale.		X		
Il software consente l'adozione di tecniche di pseudonimizzazione in relazione alla gestione di categorie particolari di dati personali, o dati personali relativi a condanne penali o reati	X			
Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, sono trattati mediante codici identificativi che non esplicitano direttamente il contenuto informativo			X	
Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, o documenti che contengono in modo non divisibile dati personali e categorie particolari di dati personali sono trattati mediante tecniche di cifratura			X	
Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, sono trattati mediante altre soluzioni rispetto alle due precedenti, ai fini della loro temporanea inintelligibilità			X	
Diritto all'oblio	SI	NO	N.A.	NOTE
Il sistema consente di definire, per classi di informazioni, il tempo di conservazione in relazione al momento in cui sono state prodotte e al momento in cui è stata raggiunta la finalità per le quali sono state raccolte.			X	
Il sistema consente la cancellazione delle informazioni che hanno raggiunto il tempo limite di conservazione	X			Non in maniera automatica
Il sistema consente di individuare le informazioni relative ad un soggetto (interessato), e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco	X			
Il sistema dispone di servizi (esempio in collaborazione applicativa) che consentono ad un sistema esterno di individuare le informazioni relative ad un soggetto (interessato), e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco	X			Tramite API
Sezione riservata alla DPIA per: - Fascicolo Sanitario Elettronico (FSE) - Dossier Sanitario Elettronico (DSE)	SI	NO	N.A.	NOTE
Il sistema consente di rilevare e tenere traccia temporalmente dei consensi e delle cessazioni di consenso, del paziente alla consultazione del suo FSE/DSE			X	
Il sistema consente il collegamento con sistemi esterni per acquisire l'esistenza o meno del consenso del paziente alla consultazione del suo FSE/DSE			X	
Il sistema consente l'accesso al FSE/DSE solo in relazione alla preventiva definizione del mandato assistenziale attivo (visita, ricovero, ecc.) che ne giustifica l'utilizzo			X	
Il sistema consente di qualificare ogni singolo episodio di cura nello status deciso dal paziente relativamente al FSE/DSE (visibile, oscurato, oscuramento dell'oscuramento)			X	
Relativamente ai dati a maggior tutela, il sistema consente di identificarli e di rilevare lo specifico consenso del paziente ai fini del trattamento FSE/DSE			X	

Il sistema consente la visibilità dei dati alla sola struttura di appartenenza del sanitario in caso di non autorizzazione alla consultazione del FSE/DSE			X	
Il sistema tiene traccia degli accessi al FSE/DSE, rilevando i dati dell'operatore sanitario, della postazione di lavoro di accesso, della data e ora di accesso e delle azioni, anche di sola inquiry eseguite			X	
Il sistema consente l'accesso al sistema da parte del paziente tramite tessera sanitaria, al fine di operare sul proprio FSE/DSE, e di verificare chi ha effettuato accessi al proprio FSE/DSE			X	
Requisiti collegati al dispiegamento	SI	NO	N.A.	NOTE
Il software consente la gestione aziendale con i dati su database criptato		X		
Il software consente la gestione multi-aziendale con separazione fisica dei dati di ciascuna azienda		X		
Il software consente la gestione multi-aziendale con separazione logica dei dati di ciascuna azienda	X			
È effettuata la ricerca continua delle vulnerabilità sia sul codice che sulla configurazione	X			

Determinazione e descrizione delle misure generali di sicurezza

Misure generali di sicurezza del sistema dove il trattamento è effettuato	Modalità operative e giustificazioni se non previste	Accettabili (A) / migliorabili (M)?	Misure correttive
Lotta contro malware	La rete del Policlinico è dotata di sistemi antivirus, web filtering e antispam che consentono di ridurre la probabilità di diffusione di malware sia attraverso l'accesso a internet, sia attraverso il sistema di posta aziendale con opportuni filtri applicati in ambo i contesti. Gli accessi esterni alla rete aziendale (a fini manutentivi) avvengono esclusivamente attraverso VPN.	A	
Gestione delle postazioni lavoro	Le postazioni di lavoro seguono installazione standard di sistema operativo ed applicativi aziendali. Vengono applicate periodicamente le patch di sicurezza necessarie, rilasciate dal produttore del S.O. e vengono tracciati log di accesso alle postazioni di lavoro. Viene altresì suggerito l'uso di cartelle condivise su sistemi server che sono soggetti a backup.	N.A.	Accessibile dal web
Sicurezza dei siti web	Il sito web aziendale utilizza sistema di crittatura SSL/TLS ed è stato soggetto ad audit di sicurezza nel 2019 a seguito del quale si è proceduto ad aggiornamento della piattaforma CMS.	A	

Salvaguardia/backup	Vengono applicate politiche di backup dei dati aziendali ed in particolare per tutte le basi di dati aziendali su DSMS. Il backup dei dati viene conservato in una sede separata. Le policy di backup seguono diverse periodicità.	A	
Modalità di mantenimento server/sistemi/software	La manutenzione dei dispositivi è articolata in: manutenzione delle postazioni di lavoro gestita in outsourcing; manutenzione hardware dei server e degli apparati del datacenter gestita attraverso contratti di manutenzione specifici con i singoli fornitori; manutenzione degli apparati di rete e fonia gestita in outsourcing con singolo fornitore di servizi per tutta la rete campus; manutenzione sistemistica e gestione interna; manutenzione sistemistica affidata in outsourcing; manutenzione del software sviluppato internamente; manutenzione ed assistenza sul software con specifici contratti di servizio dei fornitori delle applicazioni.	A	
Criteri di complessità della password	Utilizzo di almeno 8 caratteri con criteri di complessità: almeno un maiuscolo, un numero e un carattere speciale	M	Criteri personalizzabili
Obbligatorietà del cambio password al primo accesso	Ogni volta che un utente accede per la prima volta ad un sistema deve modificare la propria password	A	Valido per utenti REDCap fuori dominio LDAP
Obbligatorietà del cambio password ogni 3 mesi	Ogni 3 mesi, la password scade e occorre modificarla	A	Valido per utenti REDCap fuori dominio LDAP
Disattivazione automatica delle credenziali dopo 6 mesi di non utilizzo	Se un utente non utilizza le proprie credenziali per un periodo > 6 mesi, le credenziali sono disattivate	A	Valido per utenti REDCap fuori dominio LDAP
Disconnessione dell'utente in caso di non uso dell'applicativo per un periodo di tempo parametrizzabile	Viene individuata una durata temporale (es. 1 minuto, 3 minuti) superata la quale l'utente viene disconnesso dall'applicativo	A	
Sicurezza dei canali informatici (reti)	Il sistema informatico del Policlinico prevede strumenti di gestione della sicurezza quali Firewall, uso del VPN, sistemi di web filtering e content filtering della posta elettronica, sistemi antivirus dei client costantemente aggiornati.	A	

Sorveglianza fisica	Sistemi di controllo accessi.	A	
Controlli degli accessi fisici	Adozione di misure volte a ridurre i rischi di accessi fisici illeciti, quali accessi unicamente a soggetti autorizzati, porte e armadi chiusi a chiave, accessi ai locali sorvegliati. Nello specifico, i locali del Datacenter e in genere i locali ritenuti critici, oltre ad essere soggetti a sistemi di controllo accessi che abilitano l'accesso esclusivamente al personale autorizzato, sono abilitati a tracciare sia gli eventi di accesso che i tentativi di accesso falliti. Le porte dei datacenter sono sempre chiuse ed eventuali ospiti o personale non autorizzato viene accompagnato dal personale abilitato della U.O. ICT.	A	
Sicurezza dei materiali	L'hardware centrale dei datacenter è selezionato in modo da garantire adeguate performance anche in termini di sicurezza. Come noto, il tasso di obsolescenza delle infrastrutture è particolarmente elevato e sono pertanto in corso azioni di migrazione di sistemi applicativi che consentano una migliore manutenibilità anche in termini di sicurezza generale (inclusa la persistenza e disponibilità dei dati). L'hardware è inventariato e l'accesso allo stesso prevede autorizzazioni specifiche. Non sono adottate al momento policy di limitazione di uso delle porte I/O dei personal computer, mentre sono adottate politiche di gestione dei dispositivi in rete che impediscano il collegamento di oggetti non precedentemente identificati.	A	
Allontanamento delle fonti di rischio	Allo stato attuale non è previsto il trasferimento dei dati al di fuori della U.E. Le policy di dominio e applicate sui PC non consentono l'installazione di applicazioni da parte degli utenti non amministratori. Le applicazioni installate sono tutte censite.	A	
Continuità operativa	Capacità di un'organizzazione di adottare, per ciascun processo o servizio critico, misure di reazione e contenimento ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi e funzioni istituzionali.	N.A.	

Descrizione delle misure organizzative (Governance) ulteriori rispetto a quelle sopra elencate, a titolo esemplificativo istruzioni operative specifiche, procedure ecc)

Misure organizzative (Governance)	Modalità operative e giustificazioni se non previste	Accettabili (A) / migliorabili (M)?	Misure correttive
Gestione del progetto (Project Management) Adozione di metodologie di Project Management, con l'obiettivo di pianificazione, organizzazione, esecuzione, monitoraggio e chiusura di un progetto, al fine di raggiungere specifici risultati entro vincoli definiti di tempo, costo e risorse	Indicare specifiche Istruzioni Operative/procedure aziendali/protocolli di riferimento	A	
Formazione obbligatoria dei soggetti delegati/autorizzati	Formazione del personale in materia di protezione dei dati personali	A	
Gestione degli incidenti e della violazione dei dati (Data Breach)	Adozione di apposita procedura aziendale al fine di gestire eventuali Data Breach.	A	
Manuale di conservazione	Adozione standard di riferimento per la corretta gestione dei tempi di conservazione dei dati	A	
Procedura gestione esercizio dei diritti	Adozione di apposita procedura aziendale al fine di gestire eventuali richieste di esercizio dei diritti relativi alla protezione dei dati personali da parte dei soggetti interessati	A	
Nomina del DPO e facoltà di coinvolgimento dello stesso in caso di necessità	Nomina del DPO del Policlinico	A	
Sicurezza dei documenti cartacei	Chiusura a chiave degli armadi dedicati alla conservazione del materiale cartaceo	A	

3.2 Valutazione del rischio: violazioni potenziali della privacy

Analisi e stima dei rischi

Rischio	Principali fonti di rischio	Impatti potenziali	Misure per ridurre gravità e probabilità	Gravità ¹	Probabilità ²
Accessi illegittimi ai dati	Errore umano, uso fraudolento e virus informatici	Distruzione o uso illecito dei dati violati	Implementazione delle misure generali di sicurezza descritte sopra	Massima	Trascurabile
Modifica non desiderata dei dati	Errore umano, uso fraudolento e virus informatici	Alterazione dei dati personali necessari alla valutazione dello stato di salute per lo studio	Implementazione delle misure generali di sicurezza descritte sopra	Massima	Trascurabile
Perdita dei dati	Errore umano, uso fraudolento e virus informatici	Alterazione dei dati personali necessari alla valutazione dello stato di salute per lo studio	Implementazione delle misure generali di sicurezza descritte sopra	Massima	Trascurabile
Altri rischi					

Valutazione dei rischi

Rischi	Accettabile/migliorabile?	Misure correttive	Gravità residuale	Probabilità residuale
Accesso illegittimo ai dati	A		Trascurabile	Trascurabile
Modifica non desiderata dei dati	A		Trascurabile	Trascurabile
Perdita dei dati	A		Trascurabile	Trascurabile
Altri				

4. Validazione del P.I.A.

4.1 Preparazione degli elementi utili alla validazione

Elaborazione della sintesi relativa alla conformità al GDPR delle misure che consentono il rispetto dei principi fondamentali

Legenda

¹ Graduazione: massima, elevata, limitata, trascurabile

² Graduazione: massima, elevata, limitata, trascurabile

Simbolo	0	1	2	3
Significato	Non applicabile	Non soddisfacente	Previste migliorie	Soddisfacente

Misure che consentono il rispetto dei principi fondamentali	Valutazione
Misure a garanzia della proporzionalità e necessità del trattamento	
Finalità: determinate, esplicite e legittime	3
Base giuridica	3
Minimizzazione dei dati: adeguati, pertinenti e limitati (necessari)	3
Qualità dei dati: esatti ed aggiornati	3
Durata della conservazione: limitata	3
Modalità di distruzione	3
Informazione agli interessati (trattamento legale e trasparente)	3
Raccolta del consenso	3
Individuazione e nomina degli eventuali Contitolari del trattamento identificati e contrattualizzati secondo modello istituzionale	0
Responsabili: identificati e contrattualizzati	3
Sub responsabili: identificati e contrattualizzati	0
Trasferimento rispetto dei vincoli in materia di trasferimento dati al di là dell'U.E.	0

Elaborazione della sintesi relativa alla conformità alle buone pratiche sulle misure che contribuiscono a contenere i rischi legati alla sicurezza dei dati

Misure che contribuiscono a contenere i rischi legati alla sicurezza dei dati	Valutazione
Misure di sicurezza riguardanti i dati oggetto di trattamento	
Cifratura	0
Pseudonimizzazione	3
Controllo degli accessi logici	3
Tracciabilità degli accessi amministrativi mediante conservazione dei log	3
Controllo di integrità dei dati	3
Procedure di backup dei dati	3
Meccanismi di replica dei dati	0
Accesso tramite SPID	0
Autenticazione a due fattori (MFA)	0
Gestione dei profili utente	3
Modalità di archiviazione	3
Misure di sicurezza generali riguardanti il sistema dove il trattamento è effettuato	
Lotta contro malware	3
Gestione delle postazioni lavoro	0
Sicurezza dei siti web	3
Salvaguardia/backup	3
Modalità di mantenimento server/sistemi/software	3
Criteri di complessità della password	2
Obbligatorietà del cambio password al primo accesso	3
Obbligatorietà del cambio password ogni 3 mesi	3

Disattivazione automatica delle credenziali dopo 6 mesi di non utilizzo	3
Disconnessione dell'utente in caso di non uso dell'applicativo per un periodo di tempo parametrizzabile	3
Sicurezza dei canali informatici (reti)	3
Sorveglianza fisica	3
Controlli degli accessi fisici	3
Sicurezza dei materiali	3
Allontanamento delle fonti di rischio	3
Continuità operativa	0
Misure organizzative (Governance)	
Gestione del progetto (Project Management)	3
Formazione obbligatoria dei soggetti delegati/autorizzati	3
Gestione degli incidenti e della violazione dei dati (Data Breach)	3
Manuale di conservazione	3
Procedura gestione esercizio dei diritti	3
Nomina del DPO e facoltà di coinvolgimento dello stesso in caso di necessità	3
Sicurezza dei documenti cartacei	3

In caso di utilizzo del software:

Misure che contribuiscono a contenere i rischi legati alla sicurezza dei dati	Valutazione
Misure di sicurezza relativo all'utilizzo del software sopra elencate	3

SINTESI DELLA VALUTAZIONE DEL RISCHIO

Per garantire una corretta valutazione di seguito vengono riportati gli impatti e la relativa descrizione.

Impatto	Descrizione dell'impatto	Valore
Basso	Gli individui non saranno impattati dalla Violazione o potrebbero essere impattati da alcuni superflui inconvenienti, che saranno in grado di superare senza alcun problema.	1
Medio	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà.	2
Alto	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà.	3
Molto alto	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare.	4

Successivamente si deve valutare la probabilità che l'impatto individuato si verifichi.

Probabilità	Descrizione della probabilità	Valore
Bassa	La minaccia / rischio non si può realizzare	1
Media	È probabile che la minaccia / rischio si realizzi	2
Alta	La minaccia / rischio si verificherà sicuramente prima o poi	3
Molto alta	La minaccia si realizzerà con certezza nel prossimo futuro	4

Definiti Impatto (I) e Probabilità (P) e moltiplicando il valore assegnato tramite la formula “I x P” (impatto X probabilità), si otterrà, il livello di rischio associato ad ogni singola minaccia.

Il DPIA, quindi si conclude con la valutazione complessiva del rischio associato alle attività di trattamento individuate. La valutazione finale sul rischio si ottiene tenendo in considerazione il valore massimo tra quelli associati alle singole minacce.

Di seguito viene riportato l'intervallo tramite cui è possibile assegnare una classificazione sul livello di rischio ottenuto al termine del DPIA.

Classificazione	Intervallo del rischio
Assenza di Rischio	Valore finale tra 0 e 1 compresi
Rischio Basso	Valore finale tra 2 e 6 compresi
Rischio Medio	Valore finale tra 7 e 11 compresi
Rischio Elevato	Valore finale tra 12 e 16 compresi

Quindi, con riferimento allo specifico trattamento oggetto della valutazione:

Rischi	Indice di rischio	Accettabile/migliorabile?
Accesso illegittimo ai dati	3	A
Modifica non desiderata dei dati	3	A
Perdita dei dati	2	A
Altri (specificare)		

Descrizione del piano d'azione (ove necessario)

Misure aggiuntive richieste	Responsabile	Tempo	Difficoltà	Stato di avanzamento

Opinione degli interessati o dei loro rappresentanti (ove raccolta):

Parere del Responsabile Protezione Dati (ove richiesto):

Luogo, li _____

IL RESPONSABILE PROTEZIONE DATI (nel caso sia stato richiesto il suo parere)

U.O. Clinica Anestesiologica e Terapia Intensiva

Responsabile del procedimento, Dott. Denise Battaglini

(firma del Responsabile del Procedimento) _____

DENISE
BATTAGLINI
Università
degli Studi di
Genova
18.03.2026
12:28:58
GMT+01:00

(firma del Validatore) _____

NICOLO' ANTONINO
PATRONITI
UNIVERSITÀ DEGLI
STUDI DI GENOVA
18.03.2026 13:45:30
GMT+01:00

18.03.2026
12:28:58
GMT+01:00

SOTTOSCRIZIONE:

Genova, li _____

IL TITOLARE DEL TRATTAMENTO (o suo delegato)

Aggiornamenti successivi:

Data	Aggiornamento