



## MODELLO VALUTAZIONE DI IMPATTO DI:

Titolo Progetto di Ricerca

*First-line therapy with Nivolumab plus Ipilimumab in combination with chemotherapy for metastatic non-small cell lung cancer: an ambispective, observational, italian, multicenter, real world study (NICReWo Trial)*

Compilatore: Dott. Andrea Luciani e dott.ssa Liana Bevilacqua

Funzione: Responsabile dell'Attività Progettuale

## Fase 1: ANALISI DEL CONTESTO

Seleziona la categoria di interessati i cui dati personali sono trattati
<p><input checked="" type="checkbox"/> <b>X Pazienti</b></p> <p><input type="checkbox"/> Familiari dei Pazienti</p> <p><input type="checkbox"/> Altro _____</p>
Per Ciascun soggetto interessato, elenca le categorie di dati strettamente necessari per condurre la ricerca scientifica
<p>PAZIENTI:</p> <p><input checked="" type="checkbox"/> <b>Dati Anagrafici</b></p> <p><input checked="" type="checkbox"/> <b>Contatti (es. telefono/mail)</b></p> <p><input type="checkbox"/> Immagini</p> <p><input checked="" type="checkbox"/> <b>Dati relativi alla salute</b></p> <p><input checked="" type="checkbox"/> <b>Dati relativi alla vita sessuale</b></p> <p>(Indicare i criteri per valutare il campione e le informazioni attese)</p> <p>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 S.C. di Oncologia Medica della ASST Ovest Milanese e ai quali è stato diagnosticato un tumore polmonare non a piccole cellule in stadio IV, al fine di condurre uno studio multicentrico, osservazionale, retrospettivo e prospettico (titolo dello studio: "Prima linea di terapia con Nivolumab più Ipilimumab in combinazione con chemioterapia per il trattamento del tumore del polmone non a piccole cellule: studio ambispettico, osservazionale, italiano, multicentrico, di real world – NICReWo").</p> <p>Si tratta di uno studio multicentrico, osservazionale, retrospettivo e prospettico su pazienti, ai quali è stato diagnosticato un tumore polmonare non a piccole cellule in IV stadio e che afferiscono alla S.C. di Oncologia Medica.</p> <p>Lo studio prevede due fasi:</p> <ol style="list-style-type: none"><li>1. Fase retrospettiva: progressiva revisione sistematica delle informazioni acquisite a partire dal 01/01/2022 fino ad oggi</li><li>2. Fase prospettica: si propone di raccogliere dati per il periodo di 2 anni dall'inizio dello studio.</li></ol> <p>La raccolta dei dati verrà eseguita tramite piattaforma (RedCap 14.0.15 - © 2024 Vanderbilt University) disponibile on-line su cui il promotore ha già fatto la sua valutazione di impatto a cui si rinvia.</p> <p>I dati verranno organizzati utilizzando tabelle, suddivise come di seguito precisato:</p> <ol style="list-style-type: none"><li>1. Informazioni relative al record paziente, prive dei dati direttamente identificativi e dei dati di contatto;</li></ol>



Versione del 10.07.2025

## 2. Informazioni sanitarie relative al record diagnosi e il percorso clinico seguito

## FAMILIARI:

- ☐ Dati Anagrafici  
☐ Contatti (es. telefono/mail)  
☐ Immagini  
☐ Dati relativi alla salute

(Indicare i criteri per valutare il campione e le informazioni attese)

---

---

**Indicare i criteri di pseudo anonimizzazione che si intende applicare sui dati identificati dei pazienti/familiari oggetto di indagine.**

Le tabelle saranno collegate per mezzo di un identificativo paziente random univoco (Codice alfanumerico costituito da 8 caratteri es: 6VHNOT#7)

La corrispondenza tra nominativo del paziente e il Codice univoco sarà registrata su file Excel separato.

I dati clinici saranno estratti manualmente, a cura di personale esperto e adeguatamente formato e inseriti nella CRF elettronica su piattaforma RedCap (versione 14.0.15 - © 2024 Vanderbilt University).

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 eCRF dovrà avere come chiave quella individuata nello step di pseudonimizzazione

Obiettivo di questa fase è assicurare la completa non collegabilità dei dati ai singoli pazienti.

I dati verranno esportati tramite il modulo "Data Export, Reports and Stats" effettuando uno shift casuale sulle date puntuali, di un valore compreso tra 0 e 364, mantenendo intatti gli intervalli di tempo relativi tra le varie date. Questi dati verranno infine anonimizzati seguendo i principi riportati nel documento "De-Identifying Government Datasets: Techniques and Governance" (NIST SP 800-188) ed in particolare ad ogni paziente verrà assegnato un ID numerico casuale (con distribuzione uniforme tra -2147483648 e +2147483647, cioè il minimo e il massimo rappresentabile sulla macchina per quel tipo di dato). La corrispondenza tra tale ID e il numero identificativo del paziente nell'Enrollment log verrà memorizzato in forma criptata (tramite algoritmo di crittografia simmetrica, e.g. AES) all'interno di uno file separato conservato sui server del Titolare, accessibile al solo PI dello studio e gestito da personale autorizzato dal Titolare.

Stante la natura e la finalità dello studio in oggetto, si ritiene opportuno conservare la tabella di correlazione per un periodo di 10 anni successivi al termine dello studio.

In seguito, si procederà con la cancellazione sicura (fisica) di tutti i supporti (principali e copie di backup) su cui sono conservati i dati anagrafici di correlazione.

**Tempi di conservazione stabiliti dal Massimario di scarto:**

Data di inizio prevista: data stimata secondo protocollo: 01 Novembre 2024. Non essendo stato possibile iniziare in quella data, lo studio inizierà non appena si renderanno di disponibili tutte le autorizzazioni/approvazioni necessarie ed infine la Deliberazione aziendale di autorizzazione allo svolgimento dello studio

**Luogo di custodia dei dati**

- ☐ Server aziendale  
☒ **Server/Archivi del Partner Promotore**  
☐ Server di terza parte  
☐ Archivio di /Servizio\_\_\_\_\_



Versione del 10.07.2025

<p>- Durata stimata dello studio osservazionale: 2 anni</p> <p>- Durata stimata del follow-up: durata massima stimata 24 mesi</p> <p>I dati in forma direttamente identificabile sono conservati a norma di legge nella documentazione clinica (ambito escluso dalla presente DPIA).</p> <p>La CRF e la tabella di correlazione contenenti i dati anagrafici e direttamente identificativi del paziente saranno conservati in modalità segregata per 10 anni dopo il termine dello studio.</p> <p>I risultati dello studio (dati anonimi) verranno conservati a tempo indeterminato.</p> <p>I dati di autorizzazione, identificazione ed accesso ai sistemi sono conservati per 10 anni.</p> <p>È fatta salva, come detto in precedenza, la conservazione dei dati personali, anche particolari, per un periodo superiore, nei limiti del termine di prescrizione dei diritti, in relazione ad esigenze connesse all'esercizio del diritto di difesa in caso di controversie.</p>	
<p><b>Rappresentare le categorie di soggetti interni all'organizzazione da autorizzare al trattamento dei dati:</b></p> <p>Personale incaricato e delegato dal Responsabile dello studio con i seguenti profili:</p> <p>ONCOLOGI, INFERMIERI, DATA MANAGER</p>	<p><b>Elencare gli Enti/società Esterne Destinatari (Registrare data e firma dell'Accordo con i Responsabili del Trattamento/Partners )</b></p> <p>ENTE PROMOTORE – Fondazione IRCCS Policlinico San Matteo– Titolare Autonomo</p>

#### Fonti

I dati dei pazienti utilizzati per le finalità dello studio sono acquisiti da:

- Cartelle cliniche dei pazienti in formato cartaceo
- Software elettronico Galileo per Cartelle cliniche in formato digitali. In dettaglio :
  - o Anagrafica dei pazienti
  - o Referti di anatomia patologica relativi a campioni cito-istologic
  - o Referti di esami di laboratorio relativi a campioni ematici
  - o Referti di indagini radiologiche

#### Finalità che rendono necessario il trattamento dei dati:

Le finalità del trattamento sono quelle di ricerca scientifica

L'obiettivo principale dello studio osservazionale no-profit è stimare l'Overall Survival (OS) e la Progression-free Survival (PFS) tra i pazienti adulti con tumore polmonare non a piccole cellule in stadio IV o recidivante che hanno iniziato nivolumab più ipilimumab in combinazione con 2 cicli di chemioterapia a base di platino in I linea, in condizioni di vita reale in Italia.

Il beneficio atteso dalla sperimentazione è quello di raccogliere dati di real-world nella pratica clinica, così da poter confrontare i risultati ottenuti rispetto ai dati presenti nello studio registrativo e verificarne quindi il livello di riproducibilità nella pratica clinica.

In questo studio verrà stimata stimare l'Overall Survival complessiva e la PFS dopo 24 mesi dall'inizio della terapia tra i pazienti con tumore del polmone non a piccole cellule in stadio IV o recidivante trattati con nivolumab più ipilimumab in combinazione con 2 cicli di chemioterapia a base di platino.



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.

**Presupposti giuridici che rendono lecito il trattamento:**

**X Consenso dell'Interessato a legittimare il trattamento dei dati dei pazienti che rientrano nella coorte prospettica e per ottenerne i risultati**

- ☐ Interesse pubblico Rilevante
- ☐ Soddisfazione di una norma di legge \_\_\_\_\_

**X Altro: Applicazione dell'art. 110 del D.lgs 196/2003 per i pazienti per la coorte retrospettiva**

Per i pazienti appartenenti alla coorte retrospettiva dello studio osservazionale NICReWo, non sarà acquisito il consenso informato individuale in virtù dell'art. 110 del D.lgs. 196/2003 (Codice Privacy), il quale consente, previa autorizzazione del Comitato Etico, il trattamento di dati personali per finalità di ricerca scientifica anche in assenza del consenso, qualora ricorrano motivi etici o motivi di impossibilità organizzativa documentata.

Tale impossibilità è pienamente giustificata nel presente contesto sulla base dei seguenti elementi:

- **Motivi etici:** i soggetti coinvolti sono pazienti oncologici già trattati o deceduti, affetti da tumore polmonare in stadio IV o recidivante. L'eventuale re-identificazione e contatto successivo per finalità informative legate alla ricerca comporterebbe un rischio concreto di stress emotivo, turbamento o danno psicologico, soprattutto se la patologia non fosse stata pienamente compresa al momento del trattamento o se la condizione clinica fosse stata particolarmente grave o terminale.
- **Motivi di impossibilità organizzativa:** la raccolta del consenso retroattivo sarebbe, nel caso specifico:
  - materialmente impraticabile, dato il tempo trascorso, la numerosità della coorte e l'assenza di recapiti aggiornati;
  - disproporzionata, in quanto richiederebbe risorse, verifiche e attività organizzative che comprometterebbero l'avanzamento della ricerca;
  - pregiudizievole per la qualità scientifica dello studio, poiché la mancata inclusione dei soggetti non contattabili genererebbe un campione incompleto e distorto, riducendo la validità delle analisi di sopravvivenza e la comparabilità con i dati registrativi.

La raccolta e l'analisi dei dati clinici avverrà nel pieno rispetto dei principi di necessità, minimizzazione e pseudonimizzazione, con utilizzo di chiavi identificative randomiche, separazione logica delle informazioni e crittografia dei dati sensibili.

## Fase 2 IDENTIFICA I TRATTAMENTI PREVISTI A RISCHIO

**X trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato**

- ☐ trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto di avvalersi di un bene o di un servizio o di continuare ad essere parte di un contratto in essere
- ☐ trattamenti che prevedono un uso sistematico dei dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il



Versione del 10.07.2025

trattamento di identificativi univoci in grado di identificare gli utenti dei servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati.

**X** trattamenti su larga scala di dati aventi carattere estremamente personale (es: vita familiare o privata o che incidono sull'esercizio di un diritto fondamentale o la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato)

**X** trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)

- ☐ trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es: IoT, sistemi di intelligenza artificiale, utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale, monitoraggi effettuati da dispositivi wearable, etc.)
- ☐ trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche
- ☐ trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento
- ☐ trattamenti di dati sensibili o relativi a condanne penali
- ☐ trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

**X** trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

## Fase 3: VALUTA LE MISURE DI SICUREZZA PRESENTI

### A. MISURE SICUREZZA PIATTAFORMA REDCAP AZIENDALE ( Non Applicabile)

MISURE ATTESE				
Accesso consentito tramite username e password personale	SI	NO	N/A	
Utilizzo di password alfanumeriche	SI	NO	N/A	
Utilizzo di password di almeno 8 caratteri	SI	NO	N/A	
Blocco automatico in caso di tentativi falliti di accesso multipli	SI	NO	N/A	
Impostazione di una password provvisoria per il primo accesso	SI	NO	N/A	
Cambio automatico della password da parte dell'operatore	SI	NO	N/A	
Logout dell'utente dopo un periodo di inattività	SI	NO	N/A	
I dati gestiti sono crittografati	SI	NO	N/A	
Implementazione di un sistema di controllo degli accessi per gli utenti che accedono al sistema IT	SI	NO	N/A	



Versione del 10.07.2025

Evitare l'uso di account utente comune (consentito solo tra utenti con uguale ruolo e responsabilità)	SI	NO	N/A	
Definizione e documentazione di una policy specifica per gestione della password	SI	NO	N/A	
Memorizzazione delle password in una forma "hash"	SI	NO	N/A	
Implementazione del sistema di autenticazione a due fattori (autenticazione forte)	SI	NO	N/A	
Ogni dispositivo soggetto ad autenticazione (autenticazione endpoint)	SI	NO	N/A	
Necessaria registrazione delle azioni degli amministratori e operatori di sistemi	SI	NO	N/A	
Nessuna possibilità di cancellazione e modifica del contenuto del file di registro	SI	NO	N/A	
Applicazione della crittografia alle unità/driver di archiviazione	SI	NO	N/A	
Accesso al sistema IT eseguito solo da sistemi e terminali pre-autorizzati	SI	NO	N/A	
Accesso wireless al sistema IT consentito solo ad utenti e per processi specifici	SI	NO	N/A	
Accesso da remoto al sistema IT sotto la supervisione di personale specifico dell'organizzazione	SI	NO	N/A	
Accesso ai dispositivi mobili tramite autenticazione a due fattori	SI	NO	N/A	

## GENERAZIONE E CONTROLLO FILE DI LOG

MISURE ATTESE				RILIEVI
Tracciamento delle operazioni in un file di log	SI	NO	N/A	
Facile esportazione dei log dall'ADS	SI	NO	N/A	
Conservazione dei log per almeno 6 mesi	SI	NO	N/A	
Creazione file di log per ogni sistema/applicazione utilizzata per trattamento dati	SI	NO	N/A	
File di log contrassegnati da data e ora	SI	NO	N/A	
Protezione file di log da manomissioni e accessi non autorizzati	SI	NO	N/A	
Creazione file di log e report sullo stato del sistema da parte del sistema di monitoraggio	SI	NO	N/A	

**B. DIRITTI IN MATERIA DI PRIVACY**

	<b>CANCELLAZIONE E ELIMINAZIONE DEI DATI</b>
1	<i>Sono definiti i criteri secondo cui selezionare e scartare i dati una volta raggiunti i termini massimi di cancellazione</i>
2	<i>Sono definite e condivise le politiche per lo smaltimento sicuro dei dati</i>
	<b>DIRITTI DEGLI INTERESSATI</b>
3	<i>Il progetto analizzato assicura il diritto alla rettifica dei dati</i>
4	<i>Il progetto analizzato assicura il tracciamento delle rettifiche eseguite</i>
5	<i>Il progetto analizzato assicura l'esportazione e portabilità dei dati in un formato di uso comune</i>
6	<i>Il progetto analizzato assicura la limitazione dell'accesso agli utenti se richiesto dall'interessato</i>
7	<i>Il progetto analizzato assicura la cancellazione definitiva dei dati di un utente</i>
8	<i>L'informativa è chiara ed accessibile agli interessati del trattamento analizzato ex art.13-14 del Reg. UE 2016/679</i>
9	<i>Il consenso. Dove acquisito, è documentabile e rintracciabile</i>
	<b>PERTINENZA E NECESSITA' DEI DATI</b>
10	<i>Compilazione e acquisizione dei dati sono strettamente necessari e proporzionati alle finalità</i>
	<b>SOLO PER ARCHIVI DIGITALI: GESTIONE / HOSTING</b>
11	<i>Il progetto analizzato assicura la gestione dei dati nell'Unione Europea</i>
12	<i>Il progetto analizzato prevede il trasferimento verso Paesi Terzi previa stipula degli accordi di garanzia ex art. 46-47 del GDPR tra le parti coinvolte.</i>

**C. RISERVATEZZA DEI DATI**

	<b>LOCALI IN CUI SONO COLLOCATI ARCHIVI, PC e SERVER</b>
1	<i>L'accesso ai locali dove sono custoditi archivi, campioni e postazioni di lavoro è consentito solo a personale autorizzato.</i>
2	<i>L'accesso agli archivi cartacea è consentito solo a personale formalmente autorizzato dotato di chiavi di accesso ai locali o alle armadiature.</i>
3	<i>I locali dove non presidiati da personale autorizzato sono dotati di misure anti -intrusione..</i>
	<b>CONTROLLO DEGLI ACCESSI E AUTENTICAZIONE ALLE RISORSE INFORMATICHE COINVOLTE NEL PROGETTO ANALIZZATO (es. PC, Server, Software ecc)</b>
4	<i>L'accesso è consentito tramite username e password personale</i>
5	<i>Utilizzo di password alfanumeriche di almeno 8 caratteri</i>
6	<i>Si attiva il blocco automatico in caso di tentativi falliti di accesso multipli</i>
7	<i>È impostata una password provvisoria per il primo accesso che viene cambiata automaticamente dall'operatore</i>
8	<i>E' previsto il Logout dell'utente dopo un periodo di inattività</i>



Versione del 10.07.2025

9	<i>E' impedita l'adozione di un account utente comune (consentito solo tra utenti con uguale ruolo e responsabilità)</i>
10	<i>Sono documentate e condivise con il personale le politiche di gestione della password</i>
11	<i>Dove previsto, le password sono salvate in una forma "hash"</i>
12	<i>E' prevista l'adozione di un sistema di autenticazione a due fattori (autenticazione forte)</i>
13	<i>I data base e le copie dei backup sono crittografati</i>
14	<i>Accesso al sistema IT è eseguito solo da sistemi e terminali pre-autorizzati</i>
15	<i>Accesso wireless al sistema IT è consentito solo ad utenti e per processi specifici</i>
16	<i>Accesso da remoto al sistema IT è consentito sotto la supervisione di personale specifico dell'organizzazione</i>
17	<i>I PC sono dotati di antivirus</i>
18	<i>L'aggiornamento del sistema antivirus avviene in modo centralizzato</i>
19	<i>La rete è protetta da firewall</i>
20	<i>Il personale è formato rispetto ai rischi informatici</i>
21	<i>In caso di dimissioni del dipendente/ricercatore il suo account viene sospeso e/o rimosso</i>
22	<i>Lo screensaver con protezione di PW si attiva automaticamente sui PC</i>
	<b>SOLO PER SOFTWARE UTILIZZATO PER L'ESTRAZIONE E CARICAMENTO DEI DATI: SICUREZZA DEL CICLO DI VITA DELLE APPLICAZIONI – Si rinvia alla valutazione del software applicativo REDCAP Precedentemente descritto</b>
23	<i>Sono dichiarate dal fornitore/partner Standard e pratiche di codifica sicure per impedire l'accesso non controllato al database.</i>
24	<i>Sono certificate da un organo di terza parte o mediante eventuali penetration test standard e pratiche di codifica sicure per impedire l'accesso non controllato al database.</i>
	<b>SOLO PER PORTALI O SITIWEB UTILIZZATI PER IL CARICAMENTO/ESTRAZIONE DEI DATI: GESTIONE RISCHIO DI INDICIZZAZIONE SUL WEB</b>
25	<i>Il sito prevede una tipologia di comunicazione protetta (https)</i>
26	<i>Non è possibile accedere alle pagine del sito/portale riservate tramite l'invio di link/url</i>
27	<i>Sono applicate misure volte a limitare l'Indicizzazione dei dati e rintracciabilità nei motori di ricerca delle pagine riservate</i>
28	<i>Sono state adottate tecniche anti-tampering dei link/url</i>

**D. INTEGRITA'**

	<b>PROCEDURE E PROTOCOLLI</b>
1	<i>Sono definiti i criteri di controllo della correttezza e completezza dei dati personali, anche in modalità non automatica</i>
2	<i>Sono previste forme di verifica a campione o regolari sulla correttezza e completezza dei dati personali</i>
	<b>SOLO PER: SOFTWARE/GESTIONALI – SI RINVIA ALLA VALUTAZIONE DI REDCAP</b>



Versione del 10.07.2025

3	<i>È assicurato con il partner o fornitore un contratto di assistenza per manutenzioni ordinarie e straordinarie di software e gestionali per la correzione di eventuali bug</i>
4	<i>Il software/gestionale genera degli alert in caso di mancata o non completa registrazione dei campi</i>
5	<i>Sono garantiti test e valutazione dei patch software in ambiente protetto prima dell'installazione</i>
6	<i>Sono generati alert in caso di errore nella digitazione dei campi di input</i>
7	<i>E' impossibile per l'utente forzare la procedura nel caso i campi obbligatori fossero omessi oppure i dati fossero errati</i>
8	<i>Sono tracciate le operazioni di rettifica o cancellazione del dato</i>

**E. DISPONIBILITA'**

	<b>LOCALI IN CUI SONO COLLOCATI ARCHIVI, PC e SERVER</b>
1	<i>Le condizioni dell'archivio garantiscono l'integrità dei documenti</i>
2	<i>La documentazione cartacea è posizionata in armadi</i>
3	<i>I PC/server sono sollevati da terra</i>
4	<i>Nei locali sono disposte misure antincendio adeguate e periodicamente controllate</i>
5	<i>Gli impianti elettrici e di climatizzazione sono periodicamente controllati</i>
6	<i>I PC/server sono dotati di gruppi di continuità</i>
	<b>PC IN DOTAZIONE</b>
7	<i>Esiste un piano di manutenzione dei PC dato in dotazione</i>
8	<i>Sono previsti e condivisi codici comportamentali per il corretto utilizzo dei PC o dispositivi affidati</i>
	<b>CARTELLE DEL SERVER e/O FASCICOLI CARTACEI</b>
9	<i>Le cartelle del server o fascicoli cartacei sono organizzati secondo criteri comuni condivisi</i>
10	<i>Esiste sempre una copia di sicurezza dei documenti cartacei o digitali prodotti</i>
	<b>SOLO PER SOFTWARE/GESTIONALI UTILIZZATO PER L'ESTRAZIONE E CARICAMENTO DEI DATI</b>
11	<i>È previsto un contratto di assistenza per manutenzioni ordinarie e straordinarie di software e gestionali</i>
	<b>SOLO PER SOFTWARE UTILIZZATO PER L'ESTRAZIONE E CARICAMENTO DEI DATI: SICUREZZA DEL CICLO DI VITA DELLE APPLICAZIONI</b>
12	<i>E' previsto il test e valutazione dei patch software prima dell'installazione in ambiente protetto.</i>
	<b>SOLO PER ARCHIVI DIGITALI: BACK UPS e PROCEDURE DI BUSINESS CONTINUITY</b>
13	<i>Si riscontra un adeguato livello di protezione fisica e ambientale per i backup</i>
14	<i>E' previsto il monitoraggio della corretta esecuzione dei backup per garantire la sicurezza</i>
15	<i>E' prevista una regolare esecuzione di backup completi (Esecuzione almeno giornaliera dei backup incrementali)</i>



Versione del 10.07.2025

16	<i>E' previsto il regolare test delle procedure di backup</i>
17	<i>Se prevista archiviazione di backup tramite servizio di terze parti: è prevista la generazione di una copia crittografata prima della trasmissione dal titolare del trattamento</i>
18	<i>E' prevista una struttura alternativa per assicurare la tempestiva gestione del piano di disaster recovery</i>
19	<i>Il piano di disaster recovery è periodicamente verificato.</i>



## Fase 4: CALCOLA IL RISCHIO

	TUTELA DEI DIRITTI	RISERVATEZZA	INTEGRITA'	DISPONIBILITA'
<i>Misure di controllo</i>	<input checked="" type="checkbox"/> ADEGUATE <input type="checkbox"/> PARZ. ADEGUATE <input type="checkbox"/> NON ADEGUATE	<input checked="" type="checkbox"/> ADEGUATE <input type="checkbox"/> PARZ. ADEGUATE <input type="checkbox"/> NON ADEGUATE	<input checked="" type="checkbox"/> ADEGUATE <input type="checkbox"/> PARZ. ADEGUATE <input type="checkbox"/> NON ADEGUATE	<input type="checkbox"/> X ADEGUATE <input type="checkbox"/> PARZ. ADEGUATE <input type="checkbox"/> NON ADEGUATE
<b>PROBABILITÀ DI ACCADIMENTO DI INCIDENTI PRIVACY</b> <i>(Identifica un valore da 1 a 3 sulla base dell'adeguatezza delle misure presenti)</i>	1	1	1	1
<b>IMPATTO STIMATO SULL'INTERESSATO</b> <i>(Identifica un valore da 1 a 3 sulla base delle conseguenze stimate sui diritti e libertà dell'interessato)</i>	3	2	2	2
<b>RISCHIO</b> <i>(Calcola il rischio moltiplicando il coefficiente assegnato all'impatto e alla probabilità)</i>	3	2	2	2

Le procedure di backup che assicurano la disponibilità dei dati raccolti e prodotti nell'ambito della ricerca sono affidati al promotore che non segnala nella DPIA ( vedi par 6.8 della DPIA del promotore )

Commento :

Attenzione: Prima di procedere alla compilazione consulta la legenda a seguire.

**Legenda Adeguatezza delle Misure di Controllo:**

- ☐ ADEGUATE (Più del 50% delle misure attese applicabili sono soddisfatte)
- ☐ PARZIALMENTE ADEGUATE (Sono state applicate tra il 50% e il 25% delle misure attese applicabili)
- ☐ NON ADEGUATE (È stato applicato al massimo il 25% delle misure attese applicabili)

**Attenzione: Nel calcolo delle misure soddisfatte sono da sottrarre le misure N/A.**

**Legenda Probabilità:**

- 1 – Le misure di controllo sono ADEGUATE e tali da garantire la riservatezza, integrità, disponibilità e liceità dei dati personali raccolti
- 2 – Le misure di controllo sono PARZIALMENTE ADEGUATE in termini di riservatezza, integrità, disponibilità e liceità dei dati personali raccolti
- 3 – Le misure di controllo NON SONO ADEGUATE sul piano della riservatezza, integrità, disponibilità e liceità dei dati personali raccolti

**Legenda Impatto:**

- 1 – L'interessato (es. paziente, fornitore, lavoratore) non subisce in caso di incidente privacy **nessun effetto** rispetto ai diritti, agli accordi/prestazioni attese o danno alla reputazione, danno morale e/o economico
- 2 – L'interessato potrebbe essere oggetto di un **temporaneo disservizio sanato da procedure alternative** oppure **è oggetto di un controllo accessorio** (es. replica della prestazione ricevuta; ritardo nell'erogazione di una prestazione; perdita temporanea del controllo dei propri dati)
- 3 – L'interessato **potrebbe subire qualche forma di discriminazione, penalizzazione o sanzione** (es. perdite finanziarie, perdita del lavoro, pregiudizio alla reputazione, usurpazione dell'identità, danno alla salute)

**Legenda Rischio**

IMPATTO	3	6	9
	2	4	6
	1	2	3
PROBABILITA'			

VERDE: RISCHIO BASSO. Progetto sicuro

GIALLO: RISCHIO MEDIO. Progetto da tenere sotto controllo rafforzando le misure di sicurezza.

ROSSO: RISCHIO ALTO. Progetto non sicuro

**Fase 5: PARERE DEL DPO**

☐ **Necessario**

☒ **Non necessario**

(Allegare il Parere del DPO, dove richiesto)

**Data**

\_\_\_\_\_

**Firma**

\_\_\_\_\_