**Carta intestata dell'ENTE**

*Si precisa che le parti evidenziate in rosso sono quelle da completare a cura del Titolare del trattamento e del DPO dell'Ente.*

# VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (c.d. DPIA)

| | |
|---|---|
| Titolo dello studio | |
| Centro di sperimentazione | |
| Sperimentatore Principale | |
| Promotore | |
| Data di creazione | |
| DPO/RPD | |
| Parere del DPO/RPD | |

| Storico delle revisioni | | | |
|---|---|---|---|
| Versione | Data di rilascio | Motivo della revisione | Autore |
| | | | |

## 1. Titolare e Responsabile della Protezione dei Dati

Indicare il titolare del trattamento (o i titolari, ciascuno per il suo ambito di competenza), nonché il Responsabile della protezione dei dati (eventualmente, se presente, anche del promotore), con i relativi contatti.

## 2. Nozione di valutazione d'impatto

Il Data Protection Impact Assessment (DPIA) o "*valutazione di impatto sulla protezione dei dati*" rappresenta un processo, previsto dall'art. 35 del Regolamento UE 679/2016, inteso a descrivere i rischi correlati ad un trattamento dei dati personali, valutandone la necessità e proporzionalità, nonché contribuendo a gestire, attraverso l'adozione di specifiche misure, i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei propri dati personali.

## 3. Quadro normativo

- Regolamento (UE) 679/2016 (GDPR);
- D.lgs. 196/2003 e s.m.i. per effetto del D.lgs. 101/2018;
- Articolo 29 Working Party (2017), Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" in base alle disposizioni contenute nel Regolamento (UE) 679/2016;
- Provvedimento 146/2019 del Garante per la protezione dei dati personali.
- Provvedimento 298/2024 del Garante per la protezione dei dati personali.

## 4. Soggetti interessati

L'attività interessa il trattamento di dati riguardanti:

- pazienti già in precedenza assistiti presso_____;
- pazienti che hanno fornito in precedenza propri campioni biologici presso _____;

- soggetti arruolati in studi clinici o progetti di ricerca condotti presso _____;
- altro_____.

**RICHIESTA DEL CONSENSO DEGLI INTERESSATI**

☐ È stato richiesto il parere degli interessati

☐ Non è stato richiesto il parere degli interessati

**MOTIVAZIONE DELLA MANCATA RICHIESTA DEL CONSENSO DEGLI INTERESSATI**

Spiegare in dettaglio perché non si è proceduto (o non si è ritenuto di procedere) in tal senso.

## 5. Valutazione preliminare

La valutazione preliminare consente di svolgere un *assessment* completo di tutti i dati eventualmente trattati in linea con quanto disposto dall'art. 35 del GDPR, il quale prescrive la valutazione d'impatto per i trattamenti che:

- Prevedono una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- Prevedono il trattamento, su larga scala, di categorie particolari di dati personali (art. 9 GDPR) o di dati relativi a condanne penali e a reati (art. 10 GDPR);
- Prevedono la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Di talché, nel caso di sperimentazioni, al fine di valutare la necessità della DPIA, risulta quindi fondamentale valutare la sussistenza o meno di:

a. Trattamenti che sottintendono un rischio elevato di violazione dei diritti e delle libertà delle persone fisiche (interessati);

b. Trattamenti che non rientrano nei casi esclusi dalla valutazione ai sensi del paragrafo 1 dell'art. 5 GPDR;

c. Trattamenti che rientrano in una o più delle casistiche che seguono:
   - Impossibilità di raccogliere il consenso per i casi indicati dal Provvedimento Garante n. 146/2019 e artt. 110 e 110 *bis* Codice Privacy s.m.i.;
   - Valutazione di profilazione e scoring;
   - Decisioni automatizzate;
   - Monitoraggio sistematico;
   - Trattamento di dati su larga scala;
   - Combinazioni o raffronto di insiemi di dati;
   - Dati relativi a soggetti vulnerabili;
   - Uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative;
   - Trattamenti che impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio.

d. Trattamenti che il titolare ritiene, seppur non completamente rientranti in quelli *supra* descritti, meritevoli di valutazione preliminare per la possibile sussistenza di rischi elevati.

### 5.1. Descrizione del trattamento

Il trattamento oggetto di valutazione, con la presente DPIA, riguarda:

inserire descrizione dello studio e delle attività che si intendono svolgere con specifico riguardo ai dati trattati, individuando altresì:

- Le finalità del trattamento;
- Le categorie di interessati (evidenziando se gli stessi sono soggetti minori o incapaci);
- L'individuazione di rilevanza dei trattamenti di cui al precedente punto 5);
- Responsabilità connesse al trattamento (indicare tutti i soggetti coinvolti nell'attività di trattamento che hanno accesso ai dati. Ciò è finalizzato ad individuare le aree di responsabilità);

- Le categorie di dati trattati, indicando le tipologie di dati, il ciclo di vita del trattamento, nonché le risorse di supporto ai dati (sistemi operativi…).

Valutazione: _____
Commento di valutazione: _____

### 5.2. Motivi della valutazione d'impatto

La DPIA è stata realizzata per valutare i potenziali rischi che possono derivare dall'attività di _____ nei confronti degli interessati, onde poter garantire un intervento preventivo attuato per il tramite di misure di sicurezza.

L'esecuzione della DPIA è stata ritenuta necessaria in ragione:

Specificare puntualmente le ragioni di tale scelta anche tra quelle indicate nel Provvedimento del Garante n. 146/2019 (es. impossibilità di raccogliere il consenso, alto volume di dati utilizzati relativi alla salute, durata prolungata del trattamento…).

Valutazione: _____
Commento di valutazione: _____

## 6. Conduzione della DPIA

### 6.1. Metodo adottato e standard applicabili al trattamento

Per ogni trattamento indicare il metodo adottato, nonché eventuali standard, procedure o certificazioni applicabili al trattamento ai sensi dell'art. 40 e 42 GDPR.

### 6.2. Valutazione di necessità e proporzionalità del trattamento

Al fine di valutare la necessità e proporzionalità del trattamento in relazione alle finalità è necessario:

- Illustrare se le finalità del trattamento sono specifiche, esplicite e legittime;
- Presentare le basi giuridiche del trattamento (es. consenso dell'interessato…);
- Indicare le ragioni per cui i dati raccolti sono necessari per le finalità del trattamento (e specificare che i dati raccolti sono adeguati, pertinenti e

limitati a quanto è necessario in relazione alle finalità per cui sono trattati, c.d. limitazione dei dati);

- Descrivere le misure adottate per assicurare l'accuratezza dei dati (di conseguenza, se i dati sono esatti ed aggiornati);
- Specificare la durata della conservazione ed indicare che la stessa è giustificata da ragioni giuridiche e/o dalla necessità del trattamento.

Valutazione: _____
Commento di valutazione: _____

### 6.3. Misure a tutela degli interessati

- Indicare come sono informati gli interessati (es. informative, moduli, impossibilità di informare…);
- Specificare se gli interessati possono esercitare i diritti di cui agli artt. 15 e ss. (elencare le modalità attraverso le quali gli interessati possono esercitare ad esempio il diritto di accesso, di oblio, di limitazione/opposizione. Può essere citato il "modulo esercizi diritti interessato" se adottato. In tal caso indicare dove può essere reperito, a chi va inviato, tempi di risposta…).
- Indicare se gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto;
- Specificare se i dati sono trasferiti al di fuori dell'UE, e/o dell'EEA anche per l'archiviazione (in caso positivo, indicare i Paesi).

Valutazione: _____
Commento di valutazione: _____

### 6.4. Valutazione dei rischi

Per ogni trattamento vengono individuati gli asset direttamente o indirettamente ad esso collegati. Per ognuno di essi, il processo di analisi dei rischi esamina le

vulnerabilità, le relative minacce, e le contromisure, dirette o indirette, attuate, fornendo il livello di rischio. Tale livello tiene anche conto della probabilità e dell'impatto che l'attuazione della minaccia avrebbe sui dati personali trattati, per mezzo degli specifici asset.

In tal senso si procedere ad individuare una scala di indice dei rischi da un livello di rischio molto basso sino ad un livello molto alto.

Creare una tabella (come da esempio) con l'identificazione e valutazione dei rischi, ove viene indicata la tipologia di rischio, da un lato, e la tipologia di asset (ad es. luoghi, server…) dall'altro. Tali dati dovranno essere valutati sulla base: della DISPONIBILITÀ, RISERVATEZZA ed INTEGRITÀ.

Al fine di strutturare la valutazione dei rischi in modo congruo si deve fare riferimento alle seguenti categorie:

1) **Analisi complessiva del dell'entità del rischio**

| | PROBABILITÀ DELL'EVENTO | CONSEGUENZE | ENTITA' COMPLESSIVA DEL RISCHIO |
|---|---|---|---|
| 1 | Improbabile | Trascurabili | **Molto basso** |
| 2 | Poco probabile | Marginali | **Basso** |
| 3 | Probabile | Limitate | **Medio** |
| 4 | Molto probabile | Gravi | **Alto** |
| 5 | Quasi certo | Gravissime | **Molto alto** |

2) **Valutazione dei rischi nel caso concreto**

Nella tabella che segue inserire:

- il rischio potenziale (es. uso non autorizzato del dato, presa visione abusiva di dati, malfunzionamento del software…);

- la tipologia di asset (software, luoghi, organizzazione, storage/backup…), aggiungendo colonne sulla base degli asset considerati ed indicando al di sotto l'entità complessiva del rischio (1 molto basso; 2 basso…);
- nelle ultime tre colonne (disponibilità, riservatezza, integrità) inserire una X se risultano essere coinvolte.

| Rischio | Asset 1 | Asset 2 | Disponibilità | Riservatezza | Integrità |
|---|---|---|---|---|---|
| Es. Perdita di dati | Es. Storage/data base | | | | |
| Es. trattamento illecito o accessi non autorizzati | | Es. archivi | | | |

Valutazione: _____
Commento di valutazione: _____

### 6.5. Analisi degli impatti sui diritti e le libertà dell'interessato

Valutare gli impatti potenziali sui diritti e sulle libertà dell'interessato, considerando quanto segue:

- Scenario relativo alla perdita di riservatezza, integrità e disponibilità;
- Categoria di impatto:
  - Fisico: tutti i danni fisici/logistici che gli interessati potrebbero subire a seguito della violazione dei dati personali;

- Tecnico: tutti i danni a livello informatico che gli interessati potrebbero subire a seguito della violazione dei dati personali;
- Psicologico: tutti i danni psicologici che gli interessati potrebbero subire a seguito della violazione dei dati personali.

Per ogni categoria indicare in una tabella il livello di impatto da N.A. a massimo 4 (N.A.: non applicabile; 1: trascurabile; 2: limitato; 3: significativo; 4: massimo):

| **Livelli di impatto per categoria** | | | |
|---|---|---|---|
| Livello | Impatto fisico | Impatto tecnico | Impatto psicologico |
| N.A. (non applicabile) | Gli interessati non subirebbero alcun impatto… | Gli interessati non subirebbero alcun impatto… | Gli interessati non subirebbero alcun impatto… |
| 1 (trascurabile) | Gli interessati potrebbero incontrare… | Gli interessati potrebbero incontrare… | Gli interessati potrebbero incontrare… |
| 2 (limitato) | Gli interessati potrebbero sperimentare inconvenienti… | Gli interessati potrebbero sperimentare inconvenienti… | Gli interessati potrebbero sperimentare inconvenienti… |
| 3 (significativo) | Gli interessati potrebbero subire conseguenze… | Gli interessati potrebbero subire conseguenze… | Gli interessati potrebbero subire conseguenze… |
| 4 (massimo) | Gli interessati potrebbero sperimentare gravi… | Gli interessati potrebbero sperimentare gravi… | Gli interessati potrebbero sperimentare gravi… |

Valutazione: _____
Commento di valutazione: _____

### 7. Piano d'azione: Mitigazione dei rischi

La mitigazione dei rischi precedentemente individuati avviene applicando le seguenti misure di sicurezza a garanzia della riservatezza, disponibilità ed integrità dei dati a livello:

a. Organizzativo, tramite: indicare gli interventi svolti (ad es. predisposizione modello organizzativo privacy, assegnazione di incarichi a personale qualificato, predisposizione di nomine per soggetti esterni responsabili del trattamento, formazione in merito al trattamento…);
b. Fisico, tramite: indicare gli interventi svolti (ad es. gestione degli accessi alle sedi di trattamento, dispositivi di allarme…);
c. Tecnico/informatico, tramite: indicare gli interventi svolti (ad es. misure di sicurezza informatiche, gestione delle credenziali di accesso a sistemi e software, gestione dei log degli accessi…).

Indicare ulteriori misure eventualmente adottate, alla luce della valutazione del rischio effettivo.

In tal senso si procederà a:

- Evitare il rischio, rinunciando ad alcune delle attività che lo generano;
- Condividere il rischio con un'altra parte che sia in grado di gestirlo in modo più efficace;
- Ridurre il rischio ad un livello ritenuto accettabile, per il tramite di contromisure;
- Accettare il rischio se non si ritiene opportuna nessuna delle precedenti possibilità.

Valutazione: _____
Commento di valutazione: _____

## 8. Risultato della DPIA

Tutto ciò valutato e considerato che:

precisare in relazione alle specificità del trattamento in esame quale grado di rischio presenti allo stato attuale per i diritti e le libertà degli interessati al trattamento stesso, espresso secondo la scala di valutazione dei rischi adottata.

| **Risultati della valutazione d'impatto** | |
|---|---|
| ☐ **Rischio residuo elevato** | ☐ **Rischio residuo non elevato** |
| Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non sono ritenute sufficienti. Il rischio residuale per i diritti e le libertà degli interessanti resta elevato. | Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento sono ritenute sufficienti. |

Il Titolare del trattamento – a seguito dei risultati della DPIA - pertanto dichiara (selezionare una delle seguenti alternative):

descrivere considerazioni finali DPIA

Data _____

Firma del Titolare del trattamento _____

Data _____

Firma del Validatore/DPO _____

Allegati eventuali (*da predisporre qualora ci fossero considerazioni ulteriori che rivelano informazioni riservate di qualsiasi tipo e che pertanto l'Ente non intende pubblicare nella DPIA*):

A - Richiesta di parere al Responsabile per la Protezione dei Dati

B - Parere del Responsabile per la Protezione dei Dati

## C - Comunicazioni di aggiornamento rese al Responsabile per la Protezione dei Dati (eventuale)

Ulteriori valutazioni dello Sperimentatore Principale _____

Ulteriori valutazioni del Promotore _____