# Valutazione d'impatto sulla protezione dei dati DPIA

| | |
|---|---|
| **NOME DEL PROGETTO:** | Studio ENLIGHT |
| **DESCRIZIONE DEL PROGETTO:** | gestione di dati anonimi acquisiti da cartelle cliniche tramite cloud |

| | |
|---|---|
| Responsabile elaborazione DPIA: | Stefania Gastaldi |
| Presidente dell'Ente | Barbara Mangiacavalli |
| Redatta in collaborazione con il Responsabile della Protezione dei Dati e del responsabile del Trattamento | |

## Sommario



## ALLEGATI:

AL.01 - Protocollo Studio retrospettivo ENLIGHT_OSPEDALI
AL.02 - Supporto sulla Valutazione di Impatto Studio ENLIGHT
AL.03 - Caratteristiche Servizi Server presso Iriseos
AL.04 - Caratteristiche LimeSurvey su Server presso Iriseos
AL.05 - Carateristiche Nextcloud su Server presso Iriseos

## Premessa

Lo studio ENLIGHT è stato ideato per esplorare e analizzare i dati clinici anonimi raccolti da diverse strutture ospedaliere, con l'obiettivo di migliorare la comprensione delle patologie trattate e ottimizzare i percorsi di cura. L'approvazione da parte del Comitato Etico garantisce che lo studio sia condotto secondo rigorosi standard etici e normativi, in linea con il Regolamento UE 2016/679 (GDPR) e altre normative pertinenti in materia di protezione dei dati personali. Poiché sussistono condizioni di impossibilità organizzativa perchè contattare gli interessati implicherebbe uno sforzo sproporzionato vista la elevata numerosità del campione consistente nella totalità dei ricoveri di alcune Unità Operative di ospedali maggiori, sia quelli derivanti dalla circostanza, che all'esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto pubblicamente accessibili) essi risultino al momento dell'arruolamento nello studio, deceduti o non contattabili. Resto ferma comunque la condizioni di anonimizzazione di tali dati alla fonte.

## Sezione 0 - Verifica preliminare di applicabilità della DPIA,

In conformità all'articolo 35, del R.U. 679/2016 si è stabilito di procedere alla DPIA in quanto il trattamento in caso di violazione dei dati può avere un impatto negativo sulla protezione dei dati stessi, nonché la riservatezza e i diritti o i legittimi interessi degli interessati coinvolti

# Sezione 1 - Avvio della valutazione

| 1.1 traccia del progetto [1] |
|---|
| L'obiettivo principale dello studio ENLIGHT è quello di raccogliere e analizzare dati clinici anonimi al fine di:<br>1. Migliorare la qualità dell'assistenza sanitaria attraverso l'analisi dei dati clinici.<br>2. Identificare tendenze e pattern nei trattamenti e negli esiti dei pazienti.<br>3. Supportare lo sviluppo di linee guida cliniche basate su evidenze reali.<br>4. Contribuire alla ricerca scientifica mediante la condivisione di risultati aggregati. |

| 1.2 valutazione preliminare dell'utilizzo dei dati [2] |
|---|

| 1.2.2 Come i dati verranno raccolti? |
|---|
| I dati clinici prospettici saranno raccolti tramite survey dedicate utilizzando la piattaforma LimeSurvey, mentre i dati retrospettivi saranno acquisiti in formato esportabile anonimizzato attraverso un portale cloud basato su Nextcloud |

| 1.2.3 Chi avrà accesso ai dati? [3] |
|---|
| Autorizzati formalmente nominati e Responsabili specificatamente Incaricati |

| 1.2.4 In che modo i dati verranno trasferiti a soggetti terzi? |
|---|
| I dati non saranno trasferiti a soggetti Terzi. |

[1] Nota: esaminate le finalità del progetto in modo da esser certi di conoscere gli obiettivi e l'impatto potenziale. Probabilmente esiste già un documento introduttivo cui fare riferimento. Se no, coinvolgere il personale e tutti i terzi coinvolti nel progetto

[2] Nota: rispondete alle domande seguenti in modo che vi sia una chiara comprensione di come le informazioni verranno utilizzate, chi le userà eccetera. Ricordatevi che sono i dati personali di specifici soggetti che devono attrarre la vostra attenzione. Se non siete in grado di rispondere adesso a tutte le domande, scrivete almeno ciò che già conoscete

[3] Nota: descrivete tutti i soggetti cui i dati potrebbero essere trasferiti e analizzatene il livello di accesso. Potrebbe essere utile creare un diagramma di flusso che illustri come i dati vengono trasferiti dal punto di raccolta ad altri soggetti coinvolti

| 1.2.5 Come i dati verranno archiviati, aggiornati ed eliminati quando non più necessari ? [4] |
|---|
| I dati raccolti saranno archiviati su un server remoto gestito da IRIDEOS, conforme agli standard di sicurezza ISO/IEC 27001. Il server utilizza crittografia per proteggere i dati sia in transito che a riposo. Al termine dello studio gli stessi saranno conservati su dispositivo esterno crittografato nei tempi previsti per le pubblicazioni scientifiche. |

| 1.3 analisi preliminare dei soggetti coinvolti [5] |
|---|
| Ente Titolare, Responsabili Esterni e Fornitore di Servizi |

| 1.4 analisi di contesti precedenti e similari [6] |
|---|
| N/A |

| | | | |
|---|---|---|---|
| Sezione 1 completata da: | Responsabile Uff. Privacy | Data: | 20/06/2024 |

[4] Nota: attenzione al fatto che queste domande fanno riferimento a tutti coloro che hanno accesso ai dati. Attenzione particolare alle normative europee per cancellare dati cartacei ed informatici

[5] Nota: questa analisi deve fare riferimento a tutti coloro che sono coinvolti nel progetto ed anche a coloro che potrebbero essere coinvolti, seppure di riflesso. È meglio compilare, questo punto, una lista la più ampia possibile, che potrà essere ridotta successivamente, quando l'indagine diventerà sempre più focalizzata

[6] Nota: in questa fase è opportuno raccogliere informazioni su progetti precedenti, di natura similare, sviluppatisi all'interno, sia all'esterno dell'ente. Questa indagine può essere utile per acquisire preziose informazioni su problemi e soluzioni incontrate in precedenza. C'è sempre da imparare dalle esperienze altrui

## Sezione 2 - Impostazione dell'analisi di rischio preliminare [7]

| |
|---|
| Le domande che seguono permettono di assumere una decisione circa il fatto che sia o meno appropriata lo sviluppo di una DPIA e il livello di approfondimento della stessa , anche in casi dove tale DPA non è obbligatoria |

### 2.1 Tecnologie utilizzate
**Redatto su informazioni del Responsabile del trattamento e del Fornitore**

| **2.1.1 in questo progetto verranno utilizzate nuove tecnologie informatiche che potrebbero avere un significativo potenziale di violazione della protezione dei dati personali e riduzione del livello di protezione dei dati, che bisogna garantire agli interessati?** |
|---|
| Si, ma al fine di minimizzare il rischio il Responsabile e il fornitore della piattaforma hanno messo a disposizione dei Documenti per aiutare la valutazione di impatto che lo rende conforme al GDPR. |

### 2.2 Metodi di identificazione
**Redatto su informazioni del Fornitore**

| **2.2.1 verranno utilizzati nuovi metodi di identificazione dei dati o verranno riutilizzati identificatori già esistenti ed in uso?** |
|---|
| Sara generato un sistema di autenticazione univoco con chiave crittografata a doppia Autenticazione |

| **2.2.3 verranno utilizzati nuovi o significativamente modificati requisiti di autentica di identità, che possono risultare intrusivi od onerosi?** |
|---|
| No al momento non sono previste implementazioni |

### 2.3 Coinvolgimento di altre strutture
**Redatto su informazioni dell'Ente**

| **2.3.1 Questa iniziativa di trattamento coinvolge altre strutture, sia pubbliche, sia private, sia appartenenti a settori non-profit e volontari?** |
|---|
| Si – Ospedali che parteciperanno al progetto |

[7] nota: una analisi di rischio è sempre necessaria, per decidere se una DPIA è obbligatoria o raccomandata

## 2.4 Modifiche alle modalità di trattamento dei dati

| **2.4.1 Questa iniziativa di trattamento apporterà nuove o significative modifiche alle modalità di trattamento dei dati personali, che potrebbero destare preoccupazioni nell'interessato? [8]** |
|---|
| Si |

| **2.4.2 i dati personali, afferenti ad un interessato, già presenti in un esistente data base, verranno assoggettati a nuove o modificate modalità di trattamento?** |
|---|
| No |

| **2.4.3 i dati personali, afferenti ad un gran numero di interessati, verranno assoggettati a nuove o significative modifiche delle modalità di trattamento?** |
|---|
| no |

| **2.4.4 questa iniziativa di trattamento apporterà nuove o significative modifiche alle modalità di consolidamento, interscambio, riferimenti incrociati, abbinamento di dati personali, provenienti da più sistemi di trattamento?** |
|---|
| No |

## 2.5 Modifiche alle procedure di trattamento dei dati

| **2.5.1 questo trattamento potrà introdurre nuove modalità e procedure di raccolta dei dati, che non siano sufficientemente trasparenti o siano intrusive?** |
|---|
| No |

| **2.5.2 questo trattamento potrà introdurre modifiche a sistemi e processi, appoggiati a normative in vigore, che possano avere esiti non chiari o non soddisfacenti?** |
|---|
| No |

| **2.5.3 questo trattamento potrà introdurre modifiche a sistemi e processi, che modifichino il livello di sicurezza dei dati, in modo da portare ad esiti non chiari o non soddisfacenti?** |
|---|
| No |

| **2.5.4 questo trattamento potrà introdurre nuove o modificate procedure sicure di accesso ai dati o modalità di comunicazione e consultazione, che possano essere non chiare o permissive?** |
|---|
| No |

[8] nota: queste modifiche potrebbero riguardare le origini razziali ed etniche, le opinioni politiche, i dati sanitari, la vita sessuale, trascorsi giudiziari nonché informazioni finanziarie, che potrebbero consentire un furto di identità

| |
|---|
| **2.5.5 questo trattamento introdurrà nuove o modificate modalità di conservazione dei dati, che possano essere non chiare o prolungate oltremodo?** |
| No |

| |
|---|
| **2.5.6 questo trattamento modificherà le modalità di messa a disposizione di dati pubblicamente disponibili, in modo tale che i dati diventino più accessibili, in quanto non avveniva in precedenza?** |
| No |

## 2.6 Giustificazioni per l'avvio del progetto di trattamento

| |
|---|
| **2.6.1 le giustificazioni per l'avvio del trattamento includono contributi significativi a misure in grado di migliorare il livello della sicurezza pubblica?** |
| Si |

| |
|---|
| **2.6.2 si prevede di sviluppare una consultazione pubblica?** |
| No |

| |
|---|
| **2.6.3 la giustificazione per il nuovo progetto di trattamento dei dati è sufficientemente chiara e sufficientemente pubblicizzata?** |
| Si |

| | | | |
|---|---|---|---|
| Sezione 2 completata da: | Responsabile Uff. Privacy | Data: | 20/06/2024 |

# Sezione 3 - Esito dell'analisi preliminare dei rischi

| 3.1 Identificazione preliminare dei rischi |
|---|
| Analizzando la documentazione rilasciata dal Responsabile del Trattamento e da i Fornituri dei servizi si è verificata la conformità alle norme vigenti. (Vedere Allegati) |

| 3.2 Decisione su come procedere [9] |
|---|
| Dalle Analisi effettuate si può procedere con l'implementazione della nuova piattaforma. |

| | |
|---|---|
| Nome di colui che ha assunto la decisione [10] | Barbara mangiacavalli - Titolare dei dati |
| Nome di altri soggetti che hanno condiviso questa decisione | Stefania Gastaldi – Responsabile ufficio Privacy<br>Marco Casati - DPO |

| | | | |
|---|---|---|---|
| Sezione 3 completata da | Responsabile Uff. Privacy | Data | 20/06/2024 |

Presidente FNOPI

Firmato digitalmente da
**Barbara Mangiacavalli**
CN = Barbara Mangiacavalli
C = IT

Responsabile Ufficio Privacy

Firmato digitalmente da
**Stefania Gastaldi**
C = IT

DPO

Marco Casati
20.06.2024 14:37:40 GMT+01:00

[9] Nota: dal lavoro sinora sviluppato, siete probabilmente in condizione di stabilire se lo sviluppo di una DPIA è obbligatorio o è solo una valutazione raccomandata. Di seguito spiegate i motivi della conclusione cui siete giunti

[10] nota: ricordate che in data controller è il soggetto che ha la responsabilità finale della decisione

# Sezione 4 - Congruità con altre leggi, codici o regolamenti[11]

| **4.1 *Indicare il provvedimento*** |
|---|
| Provvedimento del 9 maggio 2024 del Garante Nazionale sulla Protezione dei Dati<br>*"In base all'art. 110 del Codice, così come modificato dall'art. 44, comma 1-bis del d.l. n. 19 del 2 marzo 2024, il Garante è chiamato a individuare le garanzie da osservare nei casi in cui per il trattamento dei dati sulla salute di cui all'art. 9 del Regolamento per scopi di ricerca medica, biomedica ed epidemiologica, non è possibile acquisire il consenso degli interessati, ai sensi dell'articolo 106, comma 2, lettera d) del Codice.*<br>*Si osserva, inoltre che l'art. 20, commi 3 e 4 del d.lgs. 101 del 2018, ha conferito al Garante il compito di verificare la conformità al Regolamento delle disposizioni contenute nei codici di deontologia e buona condotta di cui agli allegati A.1, A.2, A.3, A.4 e A.5 al Codice, rinominandole Regole deontologiche.*<br>*Con il provvedimento n. 514 del 19 dicembre 2018 il Garante ha adottato pertanto le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica che costituiscono l'attuale allegato A.5 al Codice."*<br><br>Facciamo Specifico riferimento ai seguenti punti del provvedimento:<br>2. *Individuazione delle garanzie da applicare ai sensi dell'art. 110 del Codice*<br>3. *Promovimento delle nuove regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice* |

| | | | |
|---|---|---|---|
| Sezione 5 completata da | Responsabile Uff. Privacy | Data | 20/06/2024 |

[11] nota: elencare di seguito tutti i provvedimenti legislativi o regolamentari che si applicano alla specifica attività di trattamento ipotizzata; non dimenticare eventuali codici etici od associativi. In particolare, l'articolo 38 del regolamento sulla protezione dei dati fa specifico riferimento a codici di condotta applicabili a specifiche modalità di trattamento. Si raccomanda di leggere attentamente l'articolo 38, punto per punto, onde illustrare il provvedimento e le misure adottate per soddisfare alle indicazioni, sia vincolanti, se indicative, sia orientative, del provvedimento stesso

# Sezione 5 – Contenuti analitici della DPIA [12]

| **5.1 Descrizione analitica delle operazioni di trattamento, con indicazione delle finalità e dei legittimi interessi perseguiti dal DC** |
|---|
| 1. Delibera per l'istituzione del CERSI n. 87/2022 del 21-05-2022<br>2. Delibera per il funzionamento del CERSI n. 103/2022 del 18-06-2022<br>3. Contratto tra ente ed Erogatore del servizio<br>4. Nomina responsabili del Trattamento<br>5. Nomina Autorizzati<br>6. Aggiornamento documenti Privacy<br>7. Immissione informazioni del Segnalatore sulla nuova piattaforma. |

| **5.2 Valutazione della necessità e proporzionalità delle operazioni di trattamento, in relazione alle finalità** |
|---|
| Bassa. Lo strumento è conforme al GDPR ed è un trattamento opera su dati Anonimizzati prodotti direttamente dalle strutture Ospedaliere. |

| **5.3 Valutazione dei rischi afferenti ai diritti e alle libertà degli interessati, incluso il rischio di discriminazione connesso o rinforzato dal trattamento** |
|---|
| Basso. I soggetti che accedono al trattamento sono stati Formati e gli accessi sono a codici univoci. Inoltre i dati sono anonimizzati. |

| **5.4 Descrizione delle misure individuate per mettere sotto controllo i rischi e ridurre al minimo il volume di dati personali da trattare- DPbDefault [13]** |
|---|
| Vedere Allegati |

| **5.5 Elenco dettagliato delle salvaguardie, delle misure di sicurezza e dei meccanismi adottati per garantire la protezione dati personali, fine di dimostrare la congruità con il regolamento** |
|---|
| Vedere Allegati |

| **5.6 Indicazione generale dei limiti di tempo per procedere alla cancellazione delle diverse categorie di dati raccolti** |
|---|
| Come stabilito per le Pubblicazioni Scientifiche |

| **5.7 Illustrazione di quali procedure di data protection by design e data protection by default verranno adottate, in conformità all'articolo 23** |
|---|
| Vedere Allegati |

| **7.13 Eventuale coinvolgimento del DPO** |
|---|
| È stata chiesta la collaborazione e la consulenza del DPO per tutte le parti della presente DPIA |

| Sezione 7 completata da: | Responsabile Uff. Privacy | Data: | 20/06/2024 |
|---|---|---|---|

[12] nota: l'articolo 33, comma 3, elenca in forma analitica tutte le voci che debbono comporre la DPIA
[13] nota: si prenda buona nota anche del fatto che questo tema viene trattato nella DPbD

# Sezione 6 - Approvazione della DPIA

| 6.1 Raccomandazioni [14] |
|---|
| 1. Verifica delle procedure per la gestione del nuovo trattamento;<br>2. Verifica della formazione del Personale per il Nuovo Trattamento;<br>3. Attività di audit sugli strumenti e sui responsabili del nuovo trattamento. |

| 6.2 Approvazione [15] |
|---|
| Il Nuovo trattamento viene approvato |

| | | | |
|---|---|---|---|
| Sezione 9 completata da: | Responsabile Uff. Privacy | Data: | 20/06/2024 |

[14] nota: sulla base della analisi condotta fino a questo punto, indicate quali opzioni siete in grado di raccomandare per procedere. Se rimangono in evidenza rischi significativi, occorre illustrare quale sia il problema e perché fino adesso tale problema non è stato messo sotto controllo**. È possibile che la raccomandazione dell'estensore di questo documento sia di fermare il progetto e riesaminarlo in profondità**

[15] nota: sottolineare che la approvazione comporta anche la messa disposizione di appropriate risorse umane e materiali; è indispensabile indicare in questa casella chi ha approvato le raccomandazioni del punto 9.1 ed eventuali limitazioni e condizioni che hanno condizionato questa approvazione

# Appendice A - Lista di controllo della congruità[16]

(previsto con le esigenze di protezione dei dati)

| | Domanda | Risposta |
|---|---|---|
| **1.** | Che tipologie di dati personali devono essere trattate? | Dati Personali |
| **2.** | Sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento? | Norma di Legge D.lsg. 24/2023 |
| **3.** | Se vengono trattati speciali categorie di dati, elencati all'articolo 9 comma 1, sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento? | Non Vengono trattati dati particolari |
| **4.** | Vi sono aspetti afferenti al rispetto dell'articolo 1, comma 2, del regolamento, che protegge i diritti fondamentali e le libertà delle persone fisiche, ed in particolare il loro diritto alla protezione dei dati personali, che non siano trattati in questa DPIA? [17] | No |
| **5.** | Tutti i dati personali che verranno trattati sono coperti da garanzie di riservatezza? Se sì, come questa riservatezza viene garantita? | Si -Sicurezza IT, Formazione del personale, Documentazione Interna, Procedure, Analisi sistemi del Fornitore |
| **6.** | Come viene offerta agli interessati l'informativa in merito al fatto che i loro dati personali verranno raccolti e trattati? | Pubblicata sul sito web dell'Ente |
| **7.** | Il progetto di trattamento dei dati comporta l'utilizzo di dati personali già raccolti, che verranno utilizzati per nuove finalità? | No |
| **8.** | Quali procedure vengono adottate per verificare che le procedure di raccolta dei dati sono adeguate, coerenti e non eccessive, in relazione alle finalità per i quali i dati vengono trattati? | Campi obbligatori sul portale per i Segnalatori |
| **9.** | Con quali modalità viene verificata la accuratezza dei dati personali raccolti e trattati? | A carico del Fornitore |
| **10.** | È stato effettuato una valutazione circa il fatto che il trattamento dei dati personali raccolti potrebbe causare danno o stress agli interessati coinvolti? | Si |
| **11.** | È stato stabilito un periodo massimo di conservazione dei dati? | A norma di legge |
| **12.** | Quali misure tecniche e organizzative di sicurezza sono state adottate per prevenire qualsivoglia trattamento di dati personali non autorizzato o illegittimo? | Vedere Allegati |

| Sezione 10 completata da: | Responsabile Uff. Privacy | Data: | 20/06/2024 |
|---|---|---|---|

[16] Nota: Se le risposte a queste domande sono state già date nella sezione 1 di questo documento, fate una riferimento incrociato all'appropriata risposta

[17] nota: ricordarsi delle esenzioni previste per le finalità di sicurezza pubblica, indagini penali e simili