IRE ISTITUTO NAZIONALE TUMORI REGINA ELENA ISG ISTITUTO DERMATOLOGICO SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

DELIBERAZIONE N. **811** DEL **03/10/2024**

OGGETTO: ADOZIONE DELLA PROCEDURA PER LA CONDUZIONE DI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI – VIP (C.D. DPIA), AI SENSI DELL'ART. 35 DEL REGOLAMENO EUROPEO N. 2016/679 DEL 27 GIUGNO 2016 (GENERAL DATA PROTECTION REGULATION - GDPR)

Esercizi/o e conto / Centri/o di costo / **- Importo presente Atto: € /** **- Importo esercizio corrente: € /** Budget **- Assegnato: € -** **- Utilizzato: € -** **- Residuo: € -** **Autorizzazione n°: -** Servizio Risorse Economiche: **Giovanna Evangelista**	STRUTTURA PROPONENTE **UOSD Servizio Amministrativo Ricerca** Il Dirigente Responsabile **Andrea Scotti** Responsabile del Procedimento **Andrea Scotti** L'Estensore **Chiara Giuliani** Proposta n° DL-745-2024
PARERE DEL DIRETTORE SANITARIO Positivo Data 26/09/2024 IL DIRETTORE SANITARIO f.f. **Costanza Cavuto**	**PARERE DEL DIRETTORE AMMINISTRATIVO** Positivo Data 26/09/2024 IL DIRETTORE AMMINISTRATIVO **Laura Figorilli**

Parere del Direttore Scientifico IRE **Gennaro Ciliberto** data 20/09/2024 Positivo

Parere del Direttore Scientifico ISG ad interim **Gennaro Ciliberto** data 20/09/2024 Positivo

La presente deliberazione si compone di n° 8 pagine e dei seguenti allegati che ne formano parte integrante e sostanziale:
All. 1

Il Dirigente della UOSD Servizio Amministrativo Ricerca

Visto il decreto legislativo 30 dicembre 1992 n. 502 e successive modificazioni ed integrazioni;
il decreto legislativo 16 ottobre 2003 n. 288 e il decreto legislativo 23 dicembre 2022 n. 200 di riordino della disciplina degli Istituti di ricovero e cura a carattere scientifico;

Vista la legge regionale 23 gennaio 2006, n. 2;

Visto il decreto legislativo 10 agosto 2018 n. 101, recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati-GDPR)*";

Visto l'Atto Aziendale adottato con deliberazione n. 153 del 19.02.2019 e approvato dalla Regione Lazio con DCA n. U00248 del 2.07.2019, modificato e integrato con deliberazioni n. 1254 del 02.12.2020, n. 46 del 21/01/2021 e n. 380 del 25.03.2021, approvate dalla Direzione Salute ed Integrazione Sociosanitaria della Regione Lazio, con Determinazione n. G03488 del 30.03.2021;

Vista la deliberazione della Giunta Regionale n. 256 del 17 aprile 2024, avente ad oggetto "*Commissariamento dell'IRCCS Istituti Fisioterapici Ospitalieri (Art. 8, comma 7 bis, della legge regionale 16 giugno 1994, n. 18 e s.m.i.)*";

Visto il Decreto del Presidente della Regione Lazio n. T00087 del 07 maggio 2024, avente ad oggetto: "*Nomina del Commissario straordinario dell'IRCCS Istituti Fisioterapici Ospitalieri (Art. 8, comma 7 bis, della legge regionale 16 giugno 1994, n. 18 e s.m.i.)*";

Vista la deliberazione n. 383 del 08 maggio 2024 di presa d'atto dell'insediamento del Commissario Straordinario dell'IRCCS Istituti Fisioterapici Ospitalieri Dott. Livio De Angelis;

Viste le deliberazioni n. 212 del 16 marzo 2022 e n. 367 del 23 aprile 2024 con le quali sono stati nominati rispettivamente la Dott.ssa Laura Figorilli quale Direttore Amministrativo e la Dott.ssa Costanza Cavuto quale Direttore Sanitario f.f. degli Istituti Fisioterapici Ospitalieri;

Visto il D.M. del Ministero della Salute del 20 giugno 2024 di conferma del riconoscimento del carattere scientifico dell'IRCCS di diritto pubblico a Istituti Fisioterapici Ospitalieri (IFO) relativamente alla disciplina di "oncologia" per l'Istituto Nazionale Tumori Regina Elena (IRE) e alla disciplina di "dermatologia" per l'Istituto Santa Maria e San Gallicano (ISG);

Premesso che gli IRCCS-Istituti Fisioterapici Ospitalieri-IFO (di seguito "gli IFO") sono Istituti di Ricovero e Cura a Carattere Scientifico che, secondo standard di eccellenza, perseguono finalità di ricerca, prevalentemente clinica e traslazionale, nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari ed effettuano prestazioni di ricovero e cura di alta specialità o svolgono altre attività aventi i caratteri di eccellenza di cui all'articolo 13, comma 3, lettera d), D.lgs. 2003 n. 288;

che, al fine di perseguire le citate finalità di ricerca scientifica, gli IFO sono anche impegnati nell'attività di promozione di Studi clinici/Sperimentazioni cliniche, nell'ambito dei quali è previsto il trattamento di dati personali, anche di natura particolare (art. 9, paragrafo 2 del Regolamento (UE) 2016/679 – GDPR), dei partecipanti arruolati, effettuato in conformità all'art. 6, par. 1, lett. c), all'art. 9, par.2, lett. j), GDPR, concernente il trattamento necessario a fini di ricerca scientifica, nonché all'art. 110 bis, comma 4, D.lgs. 2003, n. 196 (Codice Privacy) in tema di riutilizzo dei dati sanitari raccolti precedentemente per finalità di cura;

Atteso che, in qualità di Titolare del trattamento dei dati (art. 7 GDPR), gli IFO sono tenuti ad adempiere agli obblighi stabiliti dal GDPR, specialmente in materia di *accountability,* di *privacy by design* e *privacy by default,* di minimizzazione anche attraverso la tecnica di pseudonimizzazione dei dati, nonché di adozione di misure tecniche e organizzative adeguate a garantire un livello altrettanto adeguato al rischio derivante dal trattamento per i diritti e le libertà delle persone fisiche;

Rilevato che, in particolare, l'art. 35 GDPR ("Valutazione d'impatto sulla protezione dei dati"), stabilisce che: "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali" e che: "Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi";

che, a tal fine, il Garante per la protezione dei dati personali – GPDP, con Provvedimento n. 467 dell'11 ottobre 2018, ha elencato in modo analitico le varie tipologie di trattamento da sottoporre obbligatoriamente a valutazione d'impatto;

che il citato Codice Privacy è stato modificato all'art. 110 con D.l. 2 marzo 2024, n. 19, convertito con modificazioni dalla L. 29 aprile 2024, n. 56 e che, alla luce di ciò, il Garante per la protezione dei dati personali – GPDP ha chiarito attraverso apposite FAQ che: "Nel caso in cui gli IRCCS fondino il trattamento dei dati raccolti per finalità di cura per ulteriori finalità di ricerca sull'art. 110-bis, comma 4 del Codice, essi devono obbligatoriamente svolgere e pubblicare la Valutazione d'impatto (VIP), sui propri siti web, in quanto tale articolo costituisce una di quelle disposizioni di legge alle quali fa riferimento l'art. 110 del Codice, prescrivendo tali ulteriori adempimenti";

Considerato che, pertanto, la citata valutazione d'impatto, anche detta "Data Protection Impact Assessment – DPIA" (di seguito "DPIA") si configura come uno strumento di *risk management* fondamentale in termini di responsabilizzazione, in quanto soccorre e sostiene

il Titolare del trattamento nel garantire ed attestare il rispetto delle prescrizioni del GDPR, nonché nel dimostrare di aver adottato misure di sicurezza, anche di natura informatica, idonee a mitigare il rischio di pregiudizi per i diritti e per le libertà fondamentali delle persone fisiche durante tutte le fasi del trattamento;

che la valutazione in merito alla gravità del rischio rispetto al contesto segue i seguenti livelli:

- Livello 1 trascurabile
- Livello 2 limitato
- Livello 3 significativo
- Livello 4 massimo

Preso atto della necessità di adottare un'apposita procedura che definisca le modalità da seguire per redigere, ove richiesto dalla natura del trattamento dei dati effettuato, una DPIA e che risulti applicabile a tutte le attività svolte dagli IFO, con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e digitali e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati, anche con il supporto di fornitori esterni;

Acquisito con nota prot. n. 10845 del 5 agosto 2024, parere favorevole del Direttore Scientifico IRE-ISG;

Considerato che le attività trattamentali svolte dagli IFO vertono su:

- Trattamento di dati personali;
- Trattamento di dati elaborati su larga scala;
- Combinazione o raffronto di insiemi di dati;
- Trattamenti di dati relativi a interessati vulnerabili;

che, in ogni caso, gli IFO si impegnano ad effettuare un periodico riesame al fine di valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati, specialmente in caso di insorgenza di variazioni del rischio rappresentato dalle attività relative al trattamento;

che, ai fini della revisione, gli IFO si impegnano ad ottenere di volta in volta ulteriori specifiche informazioni contenute negli allegati al documento DPIA ("*checklist* dati" e "*checklist* misure di sicurezza", forniti dal "Data Protection Officer" – DPO d'Istituto);

che il DPO d'Istituto ha espresso parere positivo, conservato agli atti dello scrivente Ufficio, in merito all'adeguatezza dal punto di vista privacy e di data protection del documento in parola;

Ritenuto opportuno adottare la procedura per la conduzione di una valutazione di impatto sulla protezione dei dati – VIP (c.d. DPIA), ai sensi dell'art. 35 del Regolamento Europeo n. 2016/679 del 27 giugno 2016 (General Data Protection Regulation - GDPR), che, allegata al presente atto, ne costituisce parte integrante e sostanziale (All. 1);

Attestato che il presente provvedimento, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 20/94 e successive modifiche, nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, primo comma, della legge 241/90, come modificata dalla legge 15/2005.

Propone

Per i motivi di cui in narrativa che si intendono integralmente confermati di:

- adottare la procedura per la conduzione di una valutazione di impatto sulla protezione dei dati – VIP (c.d. DPIA), ai sensi dell'art. 35 del Regolamento Europeo n. 2016/679 del 27 giugno 2016 (General Data Protection Regulation - GDPR), che, allegata al presente atto, ne costituisce parte integrante e sostanziale (All. 1).

La UOSD Servizio Amministrativo per la Ricerca curerà tutti gli adempimenti per l'esecuzione della presente deliberazione.

Il Dirigente della UOSD Servizio Amministrativo Ricerca

Andrea Scotti

Il Commissario Straordinario

Visto	il decreto legislativo 30 dicembre 1992, n. 502 e s.m.i.;
Vista	la legge regionale 23 gennaio 2006 n. 2;
Visto	il decreto legislativo 16 ottobre 2003 n. 288 e il decreto legislativo 23 dicembre 2022 n. 200 "Riordino della disciplina degli Istituti di ricovero e cura a carattere scientifico";
Visto	l'Atto Aziendale adottato con deliberazione n. 153 del 19 febbraio 2019 ed approvato dalla Regione Lazio con DCA n. U00248 del 2 luglio 2019, modificato e integrato con deliberazioni n. 1254 del 02 dicembre 2020, n. 46 del 21 gennaio 2021 e n. 380 del 25 marzo 2021, approvate dalla Direzione Salute e Integrazione Socio-sanitaria della Regione Lazio, con Determinazione n. G03488 del 30 marzo 2021;
Visto	l'art. 3 comma 6 del D.lgs. 502/92 e successive modificazioni ed integrazioni, nonché l'art. 8 comma 7 della L.R. del Lazio n. 18/94.
In virtù	dei poteri di cui alla delibera IFO n. 383 del 8 maggio 2024 inerente l'insediamento del Commissario Straordinario Dott. Livio De Angelis;
Preso atto	che il Dirigente proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 20/94 e s.m.i., nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, primo comma, della legge 241/90, come modificata dalla legge 15/2005.
Visto	il parere favorevole del Direttore Amministrativo e del Direttore Sanitario Aziendale;

ritenuto di dover procedere;

Delibera

di approvare la proposta così formulata concernente *"ADOZIONE DELLA PROCEDURA PER LA CONDUZIONE DI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI – VIP (C.D. DPIA), AI SENSI DELL'ART. 35 DEL REGOLAMENO EUROPEO N. 2016/679 DEL 27 GIUGNO 2016 (GENERAL DATA PROTECTION REGULATION - GDPR)"* e di renderla disposta.

Il Commissario Straordinario

Dott. Livio De Angelis

Documento firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

Valutazione d'impatto sulla protezione dei dati (c.d. DPIA)

IRCCS Istituti Fisioterapici Ospitalieri-IFO

INDICE

1. **INTRODUZIONE**
2. **CONTESTO NORMATIVO E PROCEDURALE DI RIFERIMENTO**
3. **ATTIVITA' OGGETTO DEL DOCUMENTO**
4. **VALUTAZIONE PRELIMINARE**
5. **CONDUZIONE DELLA DPIA**
6. **RISCHI**
7. **MITIGAZIONE DEI RISCHI**
8. **RISULTATI DPIA**
9. **REVISIONE ED AGGIORNAMENTO, CON RIESAME DI CONGRUITA' CON LE ESIGENZE DI PROTEZIONE DEI DATI**

1. INTRODUZIONE

1.1. Obiettivi del documento

La presente procedura ha lo scopo di definire le modalità da seguire, ove richiesto, per una valutazione di impatto sulla protezione dei dati personali, definita "Data Protection Impact Assessment". Il *Data Protection Impact Assessment* (per brevità anche DPIA) è uno strumento importante in termini di responsabilizzazione *(principio di accountability),* in quanto soccorre e sostiene il Titolare del trattamento non soltanto nel rispettare e far rispettare le prescrizioni del GDPR, ma anche nel dimostrare di aver adottato le misure idonee a mitigare il rischio durante tutte le fasi del trattamento. In altri termini, la Valutazione d'Impatto sulla Protezione dei Dati è una procedura di *risk management* che permette di dimostrare la conformità con le norme in materia di protezione dei dati personali europee e domestiche. Prendendo le mosse dal dettato normativo, l'art. 35 GDPR prevede testualmente che: *"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi."*

Il Garante Privacy, col Provvedimento n. 467 dell'11 ottobre 2018, elenca in modo analitico le varie tipologie di trattamento da sottoporre obbligatoriamente a valutazione d'impatto *(raggiungibile al seguente link:* Elenco delle tipologie di trattamenti soggetti al requisito di una... -

Garante Privacy*).*

1.2 Campo di applicazione

La procedura è applicabile a tutte le attività svolte dagli Istituti Fisioterapici Ospitalieri-IFO (di

seguito, il "Titolare del trattamento"), con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati (clienti, fornitori, altri soggetti terzi), anche con il supporto di fornitori esterni.

Gli studi e le ricerche condotte nell'ambito di IRCCS Istituti Fisioterapici Ospitalieri-IFO sono valutati e condotti considerando i potenziali benefici in riferimento al miglioramento dei percorsi di cura per il paziente, ai risultati attesi dalla comunità scientifica e al progresso sociale generato per l'intera collettività.

2. CONTESTO NORMATIVO E PROCEDURALE DI RIFERIMENTO

La disciplina sulla *DPIA*, contenuta nel GDPR, deve essere integrata anche da quanto specificato dal *WP29* (oggi *European Data Protection Board - EDPB*) nelle linee guida concernenti la valutazione di impatto sulla protezione dei dati, nonché dai criteri per stabilire se un trattamento possa o meno presentare un rischio privacy più o meno elevato.

In particolare, le linee guida citate ampliano l'obbligatorietà della valutazione di impatto, oltre ai casi espressamente indicati dal regolamento all´art. 35, par. 3, GDPR, anche a quelli che comportano la comunicazione di dati su larga scala tra diversi titolari e/o trattamenti sistematici di dati genetici o sanitari, tenendo conto del volume dei dati, della durata e dell'attività di trattamento.

Inoltre, il Garante Privacy, in seguito alla modifica dell'art. 110 Codice Privacy, intervenuta con D.l. 2 marzo 2024, n. 19, convertito con modificazioni dalla L. 29 aprile 2024, n. 56, ha chiarito attraverso apposite FAQ che: "*Nel caso in cui gli IRCCS fondino il trattamento dei dati raccolti per finalità di cura per ulteriori finalità di ricerca sull'art. 110-bis, comma 4 del Codice,* ***essi devono obbligatoriamente svolgere e pubblicare la Valutazione d'impatto (VIP), sui propri siti web****, in quanto tale articolo costituisce una di quelle disposizioni di legge alle quali fa riferimento l'art. 110 del Codice, prescrivendo tali ulteriori adempimenti*" e ancora "*Qualora la pubblicazione per intero della VIP possa ledere diritti di proprietà intellettuale, segreti commerciali o altro,* ***il titolare del trattamento può pubblicarla per estratto****. Il mancato adempimento di tali obblighi comporta l'applicazione di una sanzione amministrativa, ai sensi dell'art. 166, comma 1 del Codice e dell'art. 83, par. 4 del Regolamento*".

Il presente documento è, inoltre, uno strumento dedicato alla valutazione del rischio ed ha lo scopo di fornire informazioni basate sia su evidenze che su metodi di analisi, al fine di rendere agevole l'adozione di decisioni informate circa il trattamento di particolari rischi.

Le informazioni ottenute consentono, quindi, di identificare i fattori determinanti e gli eventi potenzialmente dannosi, suggerendo le azioni correttive possibili da mettere in atto per prevenire la ripetizione degli eventi stessi.

Nella prospettiva della gestione del rischio privacy, tale documento risponde al principio fondamentale dell'accountability, intesa quale dimostrazione di come il Titolare del trattamento abbia posto in essere tutte le misure di sicurezza volte a tutelare i diritti e le libertà degli interessati.

La responsabilizzazione, quale obbligo di rendere conto di ciò che si fa e ciò che si fa fare, rappresenta il fulcro della nuova frontiera della privacy, in quanto aspetto essenziale per l'esercizio di una corretta ed efficace governance.

Il Regolamento UE 2016/679 pone, altresì, la necessità di rendere conto anche dell'adozione di comportamenti proattivi, tali da "*dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR*" (artt. 23-25, in particolare, e l'intero Capo IV del GDPR).

Ne consegue, dunque, che è affidato al Titolare del trattamento dei dati il compito di decidere autonomamente le modalità, le misure di sicurezza e i limiti del trattamento stesso, nel rispetto delle disposizioni normative ed alla luce dei criteri indicati nel Regolamento UE, oltre che a quelli indicati dall'ordinamento interno (Codice Privacy - D.lgs. 196/2003, come novellato dal

D.lgs. 101/2018) e rispetto alle Linee Guida e Regole Deontologiche previste dal Garante per la Protezione dei Dati Personali.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by design and by default*" (art. 25 GDPR), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio e per impostazione predefinita le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento stesso e tutelare i diritti e le libertà degli interessati, tenendo conto del contesto complessivo ove il trattamento viene svolto e dei rischi connessi.

Fondamentali fra tali attività sono quelle relative al successivo criterio del rischio inerente al trattamento; quest'ultimo è da ritenersi, infatti, come il rischio capace di impattare negativamente sulle libertà e sui diritti degli interessati (considerando 75-77).

Tali criticità dovranno essere analizzate attraverso un apposito processo di valutazione (artt. 35 e 36 GDPR), tenendo conto dei rischi noti o ipotizzabili e delle misure tecniche, fisiche e organizzative che il Titolare ritiene di dover adottare per mitigare tali rischi.

In ossequio a tali criteri, il presente documento viene redatto in base alle tecniche ed alle modalità della norma ISO/IEC 31000:2018, "*Risk Management – Principles and guidelines*", che descrive in dettaglio il processo logico e sistematico che porta alla mitigazione e controllo dei rischi.

La ratio della scelta risiede nella necessità di conferire connotati positivi alla gestione del rischio, anche attraverso la percezione dello stesso come opportunità, mediante una lettura del pericolo quale possibilità di innovazione.

Ulteriore ed importante elemento di valutazione è il contenuto dello standard ISO/IEC 31010:2009 (*Risk Management* e *Risk Assessment Techniques*), ove vengono riportati i concetti della gestione dei rischi e le diverse tecniche atte alla loro valutazione nei diversi ambiti.

È, infine, doveroso adeguarsi alle disposizioni contenute nelle norme:

- **ISO/IEC 29134:2017 ("*Information technology — Security techniques — Guidelines for privacy impact assessment*")** che indica linee guida applicabili a tutte le tipologie di strutture, pubbliche e private, al fine di creare, organizzare ed implementare progetti GDPR compliant;
- **ISO/IEC 27002:2017 ("*Information Technology - Security techniques - Code of practice for information security controls*")** che indica le linee guida per gli standard di sicurezza delle informazioni organizzative e pratiche di gestione della sicurezza delle informazioni, compresa la selezione, l'implementazione e la gestione dei controlli;
- **ISO/IEC 27005:2018 ("*Information security risk management*")** che è in parte applicabile anche alla valutazione del rischio connesso al trattamento dei dati personali; assumono importanza determinante le appendici dedicate all'approfondimento di alcuni aspetti della gestione dei rischi e, in particolare, quella relativa al catalogo delle minacce;
- **ISO/IEC 27701:2019 ("*Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*")** che fornisce requisiti e linee guida per costruire, implementare, mantenere e migliorare costantemente un *PIMS* (*Privacy Information Management System* o sistema di gestione delle informazioni sulla privacy), sia qualora l'organizzazione operi come titolare del

Trattamento (*Data Controller*), che come Responsabile (*Data Processor*).

- **ISO 31000:2018 ("*Risk management - Principles and guidelines*")** fornisce principi e linee guida generali per la gestione del rischio ed è applicabile a tutte le tipologie di organizzazioni. La ISO 31000 può essere applicata a qualsiasi tipo di rischio e nel corso dell'intero ciclo di vita di un'organizzazione, in merito a molteplici attività come la definizione di strategie e decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e beni.

3. ATTIVITÀ OGGETTO DEL DOCUMENTO

La seguente sezione illustra la tipologia di Trattamento che la procedura "DPIA" affronta.

Trattamento di dati particolari: si tratta delle categorie particolari di dati ai sensi dell'articolo 9 del GDPR (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10.

Trattamenti di dati elaborati su larga scala: il GDPR non definisce cosa costituisca larga scala, anche se il considerando 91 fornisce alcune indicazioni. In ogni caso, il *WP29* raccomanda che i seguenti fattori, in particolare, siano considerati per determinare se il trattamento è effettuato su larga scala:

a. il numero di persone interessate, come numero specifico o come percentuale della popolazione di riferimento;
b. il volume dei dati e / o la gamma di diversi elementi di dati in corso di elaborazione;
c. la durata, o la permanenza, dell'attività di elaborazione dati;
d. l'estensione geografica delle attività di elaborazione.

Combinazione o raffronto di insiemi di dati: ad esempio, provenienti da due o più trattamenti effettuati per scopi diversi e/o da altri titolari, in modo tale da superare le ragionevoli aspettative dell'interessato.

Trattamenti di dati relativi a interessati vulnerabili: un trattamento di questo tipo di dati può richiedere una DPIA a causa del maggiore squilibrio di potere tra interessato e titolare del trattamento, nel senso che il singolo può non essere in grado di valutare il rischio derivante dal trattamento.

Trattamenti di dati relativi a soggetti interessati in IRCCS Istituti Fisioterapici Ospitalieri-IFO: L'attività di IRCCS Istituti Fisioterapici Ospitalieri-IFO interessa il trattamento di dati riguardanti:

- pazienti assistiti o presi in cura presso IFO;
- soggetti arruolati in studi clinici o progetti di ricerca già condotti o di nuova presentazione presso IFO.

Il rischio e dunque la valutazione dell'impatto può essere definito come la combinazione delle probabilità di un evento e della gravità delle sue conseguenze. Qualunque tipo di iniziativa implica potenzialmente eventi e conseguenze che rappresentano possibili benefici (elementi positivi) o minacce alla sicurezza dell'attività trattamentale posta in essere (elementi negativi).

4. VALUTAZIONE PRELIMINARE

4.1 Descrizione del trattamento

IRCCS Istituti Fisioterapici Ospitalieri-IFO mediante le figure professionali di supporto ed il proprio DPO raccolgono tutte le informazioni necessarie alla Valutazione della necessità di una DPIA.

Elemento di guida sono gli *Asset* mediante i quali operano gli IFO:

- ***Data entry***: attività di raccolta dati svolta da figure professionali con competenze tecniche, scientifiche, gestionali ed organizzative;
- ***Data registry*/archivi digitali**: sviluppo, organizzazione e gestione di registri dati/archivi digitali secondo parametri assegnati mediante piattaforme;
- **Valutazione della conformità; base giuridica/motivazione legittima del trattamento:** ai sensi dell'Articolo 9, paragrafo 2, lettera j) del Regolamento UE 2016/679 e dell'Articolo 110 del Decreto legislativo 196/2003 e s.m.i, il trattamento è necessario a fini di ricerca scientifica in conformità dell'Articolo 89.
- **Individuazione dei Soggetti che accedono ai dati:** personale interno incaricato del trattamento da parte del titolare e del responsabile PI.
- **Modalità di raccolta dei dati:** attraverso *software* specialistico che ha in *input* i dati pseudonimizzati contenuti nel *datawharehouse* aziendale e che fornisce in *output* dati aggregati.
- **Modalità di aggiornamento e eliminazione dei dati:** i dati sanitari pseudonimizzati trattati nell'ambito di IRCCS Istituti Fisioterapici Ospitalieri-IFO potranno essere aggiornati e/o cancellati a seguito di apposita richiesta da parte dell'interessato.
- **Modalità di rilascio dell'informativa agli interessati:** sono fornite direttamente all'interessato a seguito delle attività eseguite nell'ambito di IRCCS Istituti Fisioterapici Ospitalieri-IFO dal personale autorizzato. Per i tipi di studi definiti "Retrospettivi", qualora possibile, sarà fatto comunque qualsiasi ragionevole sforzo per contattare i pazienti ed ottenere il consenso informato scritto, diversamente l'art. 110 bis comma 4 del D.Lgs. 196/2003 ci permette di prescindere dal consenso espresso dell'interessato in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dagli IRCCS rispetto alla ricerca. In quest'ultimo caso, l'informativa è disponibile collegandosi alla sezione "*Informazioni privacy al paziente*" del sito.
- **Trasferimento a soggetti terzi e in Paesi extra Ue**: previsto con la sottoscrizione di clausole di adeguatezza SCC (Standard Contractual Clauses).
- **Periodo di conservazione dei dati:** i dati sanitari pseudonimizzati verranno trattati

nell'ambito di IRCCS Istituti Fisioterapici Ospitalieri-IFO per il tempo previsto dalle normative vigenti in materia di sperimentazioni cliniche e, in particolare, per un periodo non superiore a 25 anni dal momento della raccolta dei dati.

- ***Asset* a sostegno del trattamento:** *hardware*, *software*, archivi e reti sono tutti compresi nel perimetro aziendale e gestiti da personale interno anche a livello di amministrazione dei sistemi.

  Gli *asset* ricadono dunque sotto le politiche di gestione e sicurezza aziendali.

4.2 Motivi della valutazione d'impatto

La DPIA è stata realizzata per valutare i potenziali rischi che possono derivare dall'attività di IRCCS Istituti Fisioterapici Ospitalieri-IFO, per cui distinguiamo:

1. **Trattamento sicuro** = il trattamento presenta, nel complesso, un rischio basso in relazione al ciclo di vita, tipologie di dati trattati, comunicazione dei dati ecc.;
2. **Trattamento parzialmente sicuro** = il trattamento presenta, nel complesso, un rischio parzialmente basso in relazione al ciclo di vita, tipologie di dati trattati, ecc.;
3. **Trattamento marginalmente rischioso** = il trattamento presenta, nel complesso, un rischio parzialmente alto in relazione al ciclo di vita, tipologie di dati trattati, ecc.;
4. **Trattamento altamente rischioso** = il trattamento presenta, nel complesso, un rischio alto in relazione al ciclo di vita, tipologie di dati trattati, ecc.

Il Rischio del trattamento si determina in funzione della probabilità di successo di una minaccia e dell'impatto sui dati, che verrà meglio specificato qui di seguito.

5. CONDUZIONE DELLA DPIA

5.1 La Finalità di trattamento è specifica, esplicita e legittima?

La finalità del trattamento è specifica, in quanto riguarda la ricerca scientifica e la sperimentazione. La finalità del trattamento è, inoltre, esplicita, in quanto è espressamente indicata (i) nella convenzione stipulata tra gli Istituti, (ii) nel protocollo dello studio e (iii) nelle informazioni privacy relative allo studio ex art. 13 GDPR.
In conclusione, la finalità del trattamento è legittima, in quanto è sorretta da una idonea base giuridica rinvenibile nell'art. 6, par. 1, lett. c) GDPR, nonché nella deroga di cui all'art. 9, par.2, lett. j), GDPR, in quanto "il trattamento è necessario a fini di ricerca scientifica". Inoltre, risulta legittima sulla base di quanto disposto dall'ultimo comma dell'art. 110 bis del Nuovo Codice Privacy in tema di riutilizzo dei dati sanitari raccolti precedentemente per finalità di cura.

5.2 Come viene rispettato il principio di minimizzazione dei dati?

Il trattamento è limitato esclusivamente ai dati necessari al conseguimento della finalità dello Studio e garantito anche grazie all'applicazione della tecnica di pseudonimizzazione. Nello specifico, ad ogni paziente arruolato verrà assegnato un codice alfa-numerico unico che sarà associato alle informazioni anagrafiche, cliniche e ai dati sperimentali. Per l'Art. 4 n. 5) GDPR la "*pseudonimizzazione è il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e*

organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

I dati possono essere mascherati in base a delle chiavi di lettura, conservate in contenitori differenti, per cui si utilizzano due chiavi distinte: la prima per cifrare il dato, la seconda per decifrarlo.

Nella pratica, il titolare del trattamento deve individuare:

- quali variabili sono identificatori diretti (ad esempio il codice fiscale);
- quali variabili sono identificatori indiretti (ad esempio la data di nascita o di morte);
- quali variabili non è necessario prendere in considerazione nel processo di anonimizzazione del dato, in quanto non sono elementi identificativi diretti o indiretti.

È sempre **opportuno non avere più di sei o al massimo otto identificatori indiretti**: l'aumento del numero degli identificatori indiretti permette di migliorare le tecniche di incrocio e ricostruire l'interessato a cui il dato si riferisce, mentre se si ha un numero di identificatori indiretti superiore ad otto, è favorevole provvedere ad una aggregazione preliminare dei dati individuali, per poi procedere alla diffusione.

5.3 Come viene rispettato il principio di RID (Riservatezza – Integrità – Disponibilità) dei dati?

- **Riservatezza**: tale principio viene rispettato mediante misure di sicurezza tecniche, fisiche ed organizzative volte a limitare la possibilità di accedere illegittimamente nei locali dove si svolgeràl'attività sperimentale. Difatti, tali locali, all'interno dei quali saranno archiviati tutti i dati relativi alla sperimentazione, sono ad accesso controllato e riservato e la documentazione è opportunamente riposta all'interno di armadiature con chiusura a chiave. Inoltre, gli accessi logici sono regolati da un sistema *Microsoft Active Directory*, su parte degli accessi elettronici è attiva la *Multifactor Authentication* (*MFA*), mentre la MFA è attiva su tutti gli accessi VPN SSL. Infine, la sicurezza degli scambi Client/Server, Vlan/Vlan e traffico Internet è gestita attraverso un firewall perimetrale.

-Integrità: tale principio viene garantito dalla circostanza per cui i dati sono sottoposti (i) quotidianamente a backup differenziale, (ii) settimanalmente a full backup, mentre (iii) la retention è 30 giorni. Vengono archiviati tre set di nastri che contengono a rotazione l'intero repository backup, conservati in luoghi sicuri. I documenti archiviati digitalmente risiedono nel cloud, la cui sicurezza è a cura del provider. Infine, vengono utilizzati esclusivamente protocolli criptati (https) con certificati di sicurezza SSL.

- **Disponibilità**: tale principio viene rispettato mediante il sistema di backup appena descritto, soggetto a test periodici, nonché attraverso (i) un sistema di disaster recovery in cloud, (ii) la segmentazione della rete Lan in Virtual Lan e (iii) sistemi di *Vulnerability Assessment* e *Penetration Test* (*VA* e *PT*).

5.4 Misure di sicurezza esistenti

- Crittografia

Si basa sulla criptazione dei dati e delle informazioni con l'obiettivo di renderli accessibili solo a chi è autorizzato.

Nello specifico, gli IFO utilizzano il seguente sistema di crittografia: TCWA non implementa nativamente tecniche di crittografia dei dati.

- Anonimizzazione

Da un punto di vista pratico, questo obiettivo può essere ottenuto attraverso l'applicazione di diverse tecniche sostanzialmente raggruppabili in due famiglie: la prima è **la randomizzazione**, che modifica il grado di verità del dato al fine di eliminare la correlazione che esiste tra lo stesso e la persona. La generalizzazione rappresenta la seconda famiglia di tecniche di anonimizzazione e consiste nel diluire gli attributi delle persone interessate modificandone la rispettiva scala o ordine di grandezza

Nello specifico, TCWA non implementa nativamente tecniche di anonimizzazione dei dati; è possibile attraverso script sul DB andare ad eseguire anonimizzazione dei dati (set di dati o dati specifici) su richiesta del cliente o secondo le politiche dell'organizzazione.

- Pseudonimizzazione

Ad ogni paziente arruolato verrà assegnato un codice alfa-numerico unico che sarà associato alle informazioni anagrafiche, che verranno conservate separatamente, e a quelle cliniche, nonché ai dati sperimentali.

Nello specifico, TCWA non implementa nativamente tecniche di pseudonimizzazione dei dati; è possibile attraverso script sul DB andare ad eseguire anonimizzazione dei dati (set di dati o dati specifici) su richiesta del cliente o secondo le politiche dell'organizzazione.

- Partizionamento

Nello specifico, TCWA implementa il partizionamento dei dati tramite tabelle separate per la gestione delle informazioni anagrafiche e dei dati clinicamente sensibili. Dette tabelle consistono in tabelle separate sul DB Postgres dell'applicativo.

- Controllo degli accessi logici

Gli accessi sono regolati da un sistema Microsoft Active Directory, su parte degli accessi alla posta elettronica è attiva la Multifactor Authentication (MFA), come anche su tutti gli accessi VPN SSL.

Nello specifico, ad ottobre 2023, sono stati aggiornati i criteri di data policy di accesso a TCWA come di seguito indicato:

La password deve rispettare le seguenti caratteristiche:

- Deve contenere almeno un numero da 0-9
- Deve contenere almeno un carattere maiuscolo
- Deve contenere almeno un carattere speciale solo ed esclusivamente tra questi indicati: @ # $ % !
- Deve avere una lunghezza minima di 8 caratteri e massima di 16
- Il cambio password viene richiesto ogni 6 mesi.

- Tracciabilità

Tutti gli accessi sono tracciati da Active Directory, quelli autorizzati dall'esterno sono tracciati anche dal concentratore VPN.

Nello specifico, TCWA dispone di un log per il controllo degli accessi e dell'operatività sui dati. Il repository dei log è sul DB applicativo e l'accesso è consentito solo ad utenti amministratori. L'accesso ai log da parte del cliente può avvenire su richiesta specifica. Le politiche di conservazione dei log sono stabilite dal cliente.

- Sicurezza e archiviazione dei documenti digitali

I documenti archiviati digitalmente risiedono nel Cloud e, pertanto, la sicurezza è a cura del provider: (i) Infocert; (ii) DR; (iii) Telecom; (iv) Microsoft, in base alla tipologia di documentazione.

Nello specifico, TCWA garantisce la persistenza dei dati su DBMS PostgreSQL; normalmente si applicano le politiche di backup e conservazione previste dall'impianto ospite.

I documenti generati da TCWA (LDO, RSA, CCE), verranno inviati al repository aziendale per la conservazione digitale una volta attivato il repository.

- Misure anti-malware

- È utilizzata una piattaforma Cynet che fornisce, attraverso agent, sicurezza da malware e analisi comportamentale. In particolare gli IFO sono dotati di un sistema di threat prevention e rilevazione di eventi anomali: ***Protezione da malware basata sull'intelligenza artificiale (IA) e Protezione da malware derivante dall'analisi statistica***

- **Sicurezza siti web**

Vengono utilizzati esclusivamente protocolli criptati (https) con certificati di sicurezza SSL.
Gli IFO sono dotati di un sistema di threat prevention e rilevazione di eventi anomali che a***nalizza il comportamento per rilevare i processi e le applicazioni non autorizzati attraverso vari meccanismi di sicurezza, nonché un Monitoraggio in tempo reale di tutte le interazioniavviate dagli utenti.***
Analizza le attività per rilevare gli attacchi alla rete, tra cui:
Furto di credenziali basato sulla rete (ARP spoofing, DNS responder)
Movimento laterale sulla rete
Comunicazioni in uscita dannose (C2C, phishing)
Ricognizione della rete (scansione delle porte)
Esfiltrazione di dati (tunneling tramite vari protocolli)

- **Backup**

I dati sono sottoposti quotidianamente a backup differenziale, settimanalmente a full backup, la retention è 30 giorni. Vengono archiviati tre set di nastri che contengono, a rotazione, l'intero repository backup di cui sopra e conservati in luogo sicuro.
Gli IFO sono dotati di misure specifiche anti ransomware, incluse quelle di resilienza, con previsione di backup a freddo, in particolare: ***Analisi del traffico di rete, Furto di credenziali basato sulla rete (ARP spoofing, DNS responder.***

- Sicurezza dei canali informatici

La sicurezza degli scambi Client/Server, Vlan/Vlan e traffico Internet è gestita attraverso un firewall perimetrale (stateful inspection). Antivirus di ultima generazione (NGAV)

- Crea nuova misura tecnica o logica

Sito in cloud di Disaster Recovery – segmentazione della rete LAN in Virtual Lan – sistemi di vulnerability assessment (VA) e penetration test (PT).
Il cloud di cui sono dotati gli IFO è su piattaforma Azure Microsoft dove un team di esperti in cibersecurity si occupano della protezione continua dei dati anche in ambienti diversi.

5.5 Misure di sicurezza fisiche e organizzative

- Controllo degli accessi fisici

Tutti i documenti cartacei sono siti in appositi locali ad accesso controllato e riservato e tale documentazione è opportunamente riposta all'interno di armadiature con chiusura a chiave.
La squadra di CyOps monitora costantemente le telemetrie del cliente, ogni ora, ogni giorno, per tutto l'anno. La squadra gestisce eventi, avvisi, richieste dei clienti e incidenti; fornisce anche un'analisi degli avvisi e delle correlazioni con altri eventi segnalati da Cynet 360.

- Prevenzione e protezione dalle fonti di rischio umane

L'accesso ai PC avviene con credenziali strettamente personale secondo la policy aziendale.

Gli esperti di IR del gruppo di CyOps lavorano in stretta collaborazione con l'azienda per risolvere gli incidenti il più rapidamente possibile. La procedura seguita comprende la creazione di politiche personalizzate all'interno di Cynet 360 per analizzare la minaccia e determinarne la portata, oltre a fornire raccomandazioni e mitigazioni sull'endpoint, nonché per tutto l'ambiente IT e relativa sicurezza

- Formazione del personale

Ogni collaboratore che avrà accesso ai dati personali ha ricevuto specifiche istruzioni sul trattamento dei dati personali da parte del Titolare, come richiesto dal GDPR. Inoltre, gli IFO hanno intrapreso già da anni uno specifico percorso formativo in ambito privacy, attraverso corsi FAD e in presenza, con test conclusivi anonimi al fine di valutare il livello di apprendimento.

5.6 Politiche di tutela della privacy

- Nomina DPO

Il DPO è stato correttamente designato dagli IFO ed è la Società Scudo Privacy s.r.l., nella personadel Dott. Carlo Villanacci.

- Nomina persone autorizzate per designazione

Tali figure privacy sono presenti all'interno degli Istituti e sono state correttamente nominate.

- Nomina Responsabile del trattamento

Gli IFO sono dotati di una procedura per la nomina di tali figure privacy che all'occorrenza predispongono e per cui ne tengono tracciabilità.

- Elaborazione e adozione policy privacy aziendali

Gli IFO hanno adottato diverse tipologie di policy in ambito privacy tra cui: (i) policy informazioni privacy; (ii) policy password; (iii) policy chiavi; ecc.

- Registro delle attività di trattamento

Gli IFO si sono dotati di un proprio Registro delle attività di trattamento elettronico, ai sensi dell'art. 30 GDPR che costantemente aggiornano.

- Modulistica privacy

Gli IFO hanno adottato diverse tipologie di informazioni privacy ex art. 13 GDPR, tra cui le Graphic Info, affisse nei locali con maggior affluenza di interessati all'interno della struttura, le informazioni privacy take-away ed ha predisposto un apposito documento informativo.

6. RISCHI

6.1 Accesso illegittimo ai dati personali

- Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di accesso illegittimo dovesse concretizzarsi?

(i) perdita del controllo dei dati personali; (ii) limitazione dei diritti; (iii) decifratura non autorizzata della pseudonimizzazione; (iv) discriminazione; (v) perdita di riservatezza dei dati personali protetti da segreto professionale; (vi) qualsiasi altro danno economico o sociale significativo.

- Quali sono le principali minacce che potrebbero concretizzare il rischio?

(i) danni fisici; (ii) compromissione di informazioni; (iii) problemi tecnici; (iv) azioni non autorizzate; (v) attacchi di ingegneria sociale.

- Quali sono le principali fonti di rischio?

(i) fattori umani interni; (ii) fattori umani esterni.

- Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

(i) Accessi regolati da un sistema Microsoft Active Directory, sia quelli interni che esterni; (ii) MFA attiva per accessi a posta elettronica e VPN SSL; (iii) archiviazione documenti digitali in Cloud; (iv) utilizzo piattaforma anti malware; (v) utilizzo protocolli criptati (https) con certificati di sicurezza SSL; (vi) presenza di un firewall perimetrale; (vii) presenza di appositi locali per conservazione documenti cartacei in armadiature chiuse a chiave; (viii) predisposizione di apposite policy come policy password e policy chiavi.

- La Valutazione in merito alla gravità del rischio rispetto al contesto segue i seguenti livelli

Livello	Descrizione
LIVELLO 1 – TRASCURABILE	Gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente che supereranno senza difficoltà
LIVELLO 2 – LIMITATO	Gli interessati potrebbero sperimentare notevoli inconvenienti, che possono superare nonostante alcune difficoltà.
LIVELLO 3 – SIGNIFICATIVO	Gli interessati potrebbero avere conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative
LIVELLO 4 – MASSIMO	Gli interessati potrebbero avere conseguenze significative, anche irrimediabili, che potrebbero non essere superate

6.2 Modifiche indesiderata dei dati personali

- Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di modifica indesiderata dei dati dovesse concretizzarsi?

(i) perdita del controllo dei dati personali; (ii) discriminazione.

- Quali sono le principali minacce che potrebbero concretizzare il rischio?

(i) azioni non autorizzate; (ii) attacchi di ingegneria sociale.

- Quali sono le principali fonti di rischio?

(i) fattori umani interni; (ii) fattori umani esterni.

- Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

(i) archiviazione documenti digitali in Cloud; (ii) backup quotidiano, settimanale e mensili, con backup repository conservato in luogo sicuro; (iii) predisposizione di un piano di Disaster Recovery con sistemi di vulnerability assessment e penetration test.

6.3 Perdita di dati personali

- Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di perdita di dati dovesse concretizzarsi?

(i) perdita del controllo dei dati personali.

- Quali sono le principali minacce che potrebbero concretizzare il rischio?

(i) danni fisici; (ii) eventi naturali; (iii) azione non autorizzate; (v) compromissione di funzioni; (vi) attacchi di ingegneria sociale.

- Quali sono le principali fonti di rischio?

(i) fonti umane interne; (ii) fonti umane esterne; (iii) fonti non umane.

- Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

(i) archiviazione documenti digitali in Cloud; (ii) backup quotidiano, settimanale e mensili, con backup repository conservato in luogo sicuro; (iii) predisposizione di un piano di Disaster Recovery con sistemi di vulnerability assessment e penetration test; (vii) presenza di appositi locali per conservazione documenti cartacei in armadiature chiuse a chiave; (viii) predisposizionedi apposite policy come policy password e policy chiavi.

Di seguito un esempio di estratto del livello di rischio per tipologie di asset, calcolato anche sulla base di vulnerabilità indirette.

Rischio	**Software**	**Luoghi**	**Organizzazione**	**Postazioni di lavoro**	**Server**	**Apparati Rete dati**	**Storage/Backup**	**disponibilità**	**riservatezza**	**integrità**
Malfunzionamento e degrado di apparecchiature	\	\	\	\	\	\	\	\	\	\

Uso non autorizzato di apparecchiature	\	\	\	\	\	\	\	\	\	\
Furto di apparecchiature	\	\	\	\	\	\	\	\	\	\
Indisponibilità sistema informativo	\	\	\	\	\	\	\	\	\	\
Ingressi non autorizzati ai locali ad accesso ristretto	\	\	\	\	\	\	\	\	\	\
Mancanza di alimentazione elettrica	\	\	\	\	\	\	\	\	\	\
Incendio	\	\	\	\	\	\	\	\	\	\
Allagamento	\	\	\	\	\	\	\	\	\	\
Furto di dati	\	\	\	\	\	\	\	\	\	\

Modifica non autorizzata di dati	\	\	\	\	\	\	\	\	\	\
Presa visione abusiva di dati	\	\	\	\	\	\	\	\	\	\
Mancata accessibilità dei dati	\	\	\	\	\	\	\	\	\	\
Mancata conservazione dati	\	\	\	\	\	\	\	\	\	\
Malfunzionamento software	\	\	\	\	\	\	\	\	\	\
Uso non autorizzato di software	\	\	\	\	\	\	\	\	\	\
Azioni di software suscettibili di arrecare danno	\	\	\	\	\	\	\	\	\	\
Accessi non autorizzati al software	\	\	\	\	\	\	\	\	\	\
Errore nello svolgimento di mansioni	\	\	\	\	\	\	\	\	\	\
Ignoranza procedure di gestione	\	\	\	\	\	\	\	\	\	\
Guasto ai sistemi complementari	\	\	\	\	\	\	\	\	\	\

7. MITIGAZIONE RISCHI

La mitigazione dei rischi sopra riportati avviene applicando le seguenti misure di sicurezza a garanzia della riservatezza, disponibilità e integrità dei dati a livello:

1. **organizzativo**, tramite ad esempio: istruzioni interne, assegnazione degli incarichi a personale qualificato, formazione agli incaricati del trattamento, profilazione degli accessi a sedi e sistemi informatici;

2. **fisico**, tramite ad esempio: gestione degli accessi alle sedi del trattamento, dispositivi di allarme, vigilanza, dispositivi antincendio, dispositivi di controllo di umidità e temperatura, continuità dell'alimentazione elettrica;

3. **logico**, tramite ad esempio: gestione delle credenziali di accesso a sistemi e software con password policy di complessità e durata, gestione dei log degli accessi a sistemi e programmi, antivirus centralizzato, firewall perimetrali, ridondanza e virtualizzazione dell'infrastruttura informatica a supporto, backup dei dati, snapshot dei sistemi, ridondanza dei collegamenti di rete, compartimentazione logica delle reti, trasmissione

cifrata dei dati, vulnerability assessment periodici

Attività	**Attori coinvolti**	**Tempistiche**
Aggiornamento, a cadenza al minimo annuale, della sezione nel Registro delle attività di trattamento dei dati nella quale sono individuati i trattamenti effettuati dal titolare che richiedono un'analisi d'impatto	• TITOLARE • COMITATO ETICO VALUTANTE	365giorni
3.4.2 Pianificazione della specifica DPIA individuata come necessaria in relazione ai dati condivisi	• RESPONSABILE DEL PROGETTO	30 giorni
3.4.3 Elaborazione della valutazione dei rischi (analisi dei criteri di svolgimento DPIA)	• PERSONALE A SUPPORTO ASPETTI PRIVACY • DPO	30 giorni
3.4.4 Definizione delle misure di controllo, compilando il documento "DPIA e piano di trattamento dei rischi"	• RESPONSABILE DEL PROGETTO • PERSONALE INFORMATICO	15 giorni
3.4.5 Riesamina della valutazione dei rischi e delle misure di controllo all'insorgere di variazioni del rischio rappresentato dalle attività relative al trattamento ed eventuale	• DPO	30 giorni

8. RISULTATI DPIA

Tutte le valutazioni compiute sono necessarie al fine di definire il grado di rischio per i diritti e le libertà degli interessati, derivante dallo stesso trattamento, espresso secondo la scala di valutazione dei rischi adottata.

9. REVISIONE ED AGGIORNAMENTO, CON RIESAME DI CONGRUITÀ CON LE ESIGENZE DI PROTEZIONE DEI DATI

Il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento (Articolo 35, paragrafo 11 del Regolamento UE 2016/679) , per tale revisione saranno richieste ulteriori informazioni contenute negli allegati al presente atto (checklist misure di sicurezza e checklist dati).

CHECKLIST – DPIA ART. 35 GDPR

VALUTAZIONE DEL CONTESTO PRIVACY

1. NOME DELL'ENTE E UNITA' OPERATIVA*

2. NOME E QUALIFICA/RUOLO DEL COMPILATORE*

3. DENOMINAZIONE DELL'ATTIVITA' DI TRATTAMENTO SVOLTA*

4. DENOMINAZIONE DELL'AMBITO E/O CIRCOSTANZA DEL TRATTAMENTO*

5. VENGONO APPLICATE E/O OSSERVATE LINEE GUIDA/BEST PRACTICE/NORMATIVA DI SETTORE (es. UNI/ ISO / IEC; codice di condotta) *

6. CATEGORIA DI DATI TRATTATI *

Seleziona tutte le voci applicabili

- ☐ dati personali anagrafici in chiaro
- ☐ dati personali anagrafici pseudonimizzati
- ☐ dati relativi alla salute e sanitari
- ☐ dati di identificazione elettronica
- ☐ dati di identificazione finanziaria
- ☐ dati biometrici
- ☐ dati antropometrici
- ☐ dati genetici
- ☐ dati relativi all'origine razziale o etnica
- ☐ dati relativi all'orientamento sessuale
- ☐ dati relativi alla vita sessuale
- ☐ dati relativi all'appartenenza sindacale
- ☐ dati relativi alle opinioni politiche
- ☐ dati relativi alle convinzioni religiose
- ☐ dati relativi alle convinzioni filosofiche
- ☐ dati di traffico/geolocalizzazione
- ☐ dati bancari
- ☐ dati contabili ed economici
- ☐ dati fiscali
- ☐ dati assicurativi
- ☐ rilievi fotografici e di immagini
- ☐ dati giudiziari
- ☐ curriculum vitae
- ☐ dati di comunicazione elettronica
- ☐ campioni biologici

Altro: ☐

7. OPERAZIONI DI TRATTAMENTO *

Seleziona tutte le voci applicabili

- ☐ raccolta
- ☐ registrazione
- ☐ conservazione cartacea
- ☐ conservazione digitale
- ☐ organizzazione
- ☐ consultazione
- ☐ elaborazione
- ☐ selezione
- ☐ estrazione
- ☐ raffronto
- ☐ utilizzo
- ☐ interconnessione

8. QUALORA VENGA SELEZIONATA LA VOCE “INTERCONNESSIONE”, INDICARE LE PIATTAFORME UTILIZZATE

9. CANCELLAZIONE *

Seleziona tutte le voci applicabili

- ☐ siano al raggiungimento delle finalità di trattamento
- ☐ adempimento obblighi contrattuali
- ☐ obbligo legale
- ☐ sino al raggiungimento dell’interesse pubblico/esercizio pubblici poteri
- ☐ mai, previa anonimizzazione

Altro:

10. COMUNICAZIONE *

Seleziona tutte le voci applicabili

- ☐ Soggetti nominati Responsabili del trattamento ex art. 28 GDPR
- ☐ Contitolari del trattamento ex art. 26 GDPR
- ☐ Persone Autorizzate per designazione al trattamento ex art. 29 GDPR e 2-quaterdecies Codice Privacy
- ☐ Assicurazioni
- ☐ Istituti bancari
- ☐ Amministrazioni Pubbliche
- ☐ Enti previdenziali
- ☐ Autorità di Giustizia
- ☐ Servizi pubblici e sociali
- ☐ Forze dell'Ordine
- ☐ Consulenti, professionisti o terzi indicati dall'interessato

Altro: ☐

11. TRASFERIMENTO: INDICARE SE È PREVISTO UN TRASFERIMENTO VERSO ORGANIZZAZIONI INTERNAZIONALI (es: OMS; CDC; FAO; ONU)

☐

12. TRASFERIMENTO PRESSO PAESI UE/SEE

Seleziona tutte le voci applicabili

- ☐ AUSTRIA
- ☐ BELGIO
- ☐ BULGARIA
- ☐ CIPRO
- ☐ CROAZIA
- ☐ DANIMARCA
- ☐ ESTONIA

- [ ] FINLANDIA
- [ ] GERMANIA
- [ ] GRECIA
- [ ] IRLANDA
- [ ] LETTONIA
- [ ] LITUANIA
- [ ] LUSSEMBURGO
- [ ] MALTA
- [ ] PAESI BASSI
- [ ] POLONIA
- [ ] PORTOGALLO
- [ ] REPUBBLICA CECA
- [ ] REPUBBLICA SLOVACCA
- [ ] ROMANIA
- [ ] SLOVENIA
- [ ] SPAGNA
- [ ] SVEZIA
- [ ] UNGHERIA
- [ ] ITALIA
- [ ] ISLANDA
- [ ] LIECHTENSTEIN
- [ ] NORVEGIA

13. TRASFERIMENTO PRESSO PAESI EXTRA UE

Seleziona tutte le voci applicabili

- [ ] ANDORRA
- [ ] ARGENTINA
- [ ] AUSTRALIA PNR
- [ ] CANADA

☐ FAER OER

☐ GIAPPONE

☐ GUERNSEY

☐ ISOLA DI MAN

☐ ISRAELE

☐ JERSEY

☐ NUOVA ZELANDA

☐ REGNO UNITO

☐ SVIZZERA

☐ URUGUAY

☐ USA PNR

14. ALTRI PAESI EXTRA UE (inserimento manuale paese non ricompreso nell'elenco precedente)

15. CONDIZIONI APPLICABILI

Seleziona tutte le voci applicabili

☐ Clausole contrattuali standard adottate dalla Commissione UE ex art. 45 GDPR

☐ Presenza di garanzie adeguate ex art. 46 GDPR

☐ Utilizzo di norme vincolanti di impresa ex art. 47 GDPR

☐ Codici di condotta ex art. 40 GDPR

☐ Istituti bancari

☐ Strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche od organismi pubblici

☐ Meccanismo di certificazione ex art. 42 GDPR

☐ Deroghe ex art. 49 GDPR

16. QUANTITÀ DEI DATI PERSONALI *

Selezione solo una voce

- ☐ Da 1 a 100
- ☐ Da 100 a 1000
- ☐ Oltre i 1000

Altro: ☐

17. TIPOLOGIA DI TRATTAMENTO *

Seleziona tutte le voci applicabili

- ☐ Processi valutativi automatizzati e profilazione
- ☐ Sorveglianza sistematica
- ☐ Elaborazione dati su larga scala con conseguenze per un gran numero di parti interessate
- ☐ Interconnessione di dati che gli interessati non possono ragionevolmente prevedere
- ☐ Monitoraggio sistematico su larga scala
- ☐ Uso di nuove tecnologie

Altro: ☐

18. PER QUANTO TEMPO VERRANNO CONSERVATI I DATI OGGETTO DI TRATTAMENTO *

Seleziona sono una voce

- ☐ Fino al raggiungimento delle finalità specifiche del trattamento
- ☐ Obbligo legale
- ☐ Tempistica prestabilita

19. QUALORA VENGA SELEZIONATA LA VOCE “OBBLIGO LEGALE”, INDICARE LA FONTE NORMATIVA E LA TEMPISTICA

☐

20. QUALORA VENGA SELEZIONATA LA VOCE “TEMPISTICA PRESTABILITA”, INDICARE IL PERIODO DI CONSERVAZIONE DEI DATI

21. INDICARE LA FINALITÀ DEL TRATTAMENTO *

Seleziona tutte le voci applicabili

- ☐ cura
- ☐ prevenzione e protezione
- ☐ studio e ricerca scientifica
- ☐ sperimentazione
- ☐ farmacovigilanza
- ☐ medicina del lavoro
- ☐ programmazione e pianificazione
- ☐ risk management
- ☐ gestione contenzioso
- ☐ gestione assicurativa- sanitaria
- ☐ organizzazione di corsi/seminari/congressi
- ☐ gestione personale
- ☐ sicurezza e protezione sui luoghi di lavoro (d. lgs. 81/2008)
- ☐ gestione fornitori/ responsabili del trattamento
- ☐ contabilità/ gestioni crediti
- ☐ emolumenti / buste paga
- ☐ gestione delle procedure amministrative
- ☐ formativa ed informativa
- ☐ acquisizione bene e servizi
- ☐ risorse economiche e bilancio
- ☐ servizi tecnici/ ICT

☐ sicurezza dei luoghi, delle persone e del patrimonio aziendale

☐ pubblicità, marketing e ricerca di mercato

☐ accesso civico (d.lgs. 33/2013)

☐ accesso amministrativo (l. 241/1990)

☐ trasparenza

☐ statistica

☐ ricerca storica

☐ amministrazione biblioteca

☐ customer care

Altro:

22. PERCHÉ I DATI PERSONALI TRATTATI SONO NECESSARI PER PERSEGUIRE LE FINALITA' DI CUI ALL'ELENCO PRECEDENTE? *

23. INDICARE LA BASE GIURIDICA CHE CONSENTE IL TRATTAMENTO DEI "DATI COMUNI" (art. 6 GDPR- es. dati anagrafici, dati bancari, dati di contatto e, comunque, tutti quei dati non ricompresi nel punto successivo) *

Seleziona tutte le voci applicabili

☐ Consenso dell'interessato

☐ Esecuzione di misure precontrattuali o di un contratto di cui l'interessato è parte

☐ Obbligo di legge al quale è soggetto il titolare del trattamento

☐ Salvaguardia interessi vitali dell'interessato o altra persona fisica

☐ Esecuzione di un interesse pubblico o trattamento connesso all'esercizio di pubblici poteri

☐ Perseguimento legittimo interesse del titolare del trattamento o di terzi

24. INDICARE LA BASE GIURIDICA CHE CONSENTE IL TRATTAMENTO DI “PARTICOLARE CATEGORIE DI DATI” (art. 9 GDPR- elenco tassativo: - dati relativi all’origine razziale o etnica; - dati biometrici; - dati genetici; - dati relativi alla salute e sanitari; - dati di appartenenza sindacale e opinioni politiche; - dati relativi alle convinzioni religiose e filosofiche; - dati relativi alla vita sessuale e all’orientamento sessuale) *

Seleziona tutte le voci applicabili

☐ Consenso esplicito dell’interessato

☐ Assolvimento obblighi e/o esercizio diritti del titolare o dell’interessato in materia di diritto del lavoro, sicurezza sociale e protezione sociale

☐ Tutela interesse vitale dell’interessato o altra persona fisica qualora l’interessato sia nell’incapacità di esprimere il proprio consenso

☐ Trattamento effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegue finalità politiche, filosofiche, religiose, sindacali a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l’associazione o l’organismo a motivo delle sue finalità e che i dati personali non siano comunicati all’esterno senza il consenso dell’interessato

☐ Trattamento relativo a dati personali resi manifestamente pubblici dall’interessato

☐ Trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria

☐ Trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell’Unione Europea o degli Stati Membri

☐ Trattamento necessario per finalità di medicina preventiva, medicina del lavoro, valutazione capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell’Unione Europea o degli Stati Membri

☐ Trattamento necessario per motivi d’interesse pubblico nel settore della sanità pubblica quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e di sicurezza dell’assistenza sanitaria e dei medicinali/ dispositivi medici sulla base del diritto dell’Unione Europea o degli Stati Membri

☐ Trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici sulla base del diritto dell’Unione Europea o degli Stati Membri

25. COME SONO RESE ALL'INTERESSATO LE INFORMAZIONI PRIVACY? *

26. OVE APPLICABILE, COME SI OTTIENE IL CONSENSO DEGLI INTERESSATI?*

27. QUALI SONO LE MODALITA' PER L'ESERCIZIO DEL DIRITTI DEGLI INTERESSATO? (quali, il diritto di accesso, di rettifica, di cancellazione, di limitazione, di portabilità dei dati, di opposizione) *

MISURE DI SICUREZZA ex art. 32 GDPR

Identità e ruolo del compilatore:

_____

Attività Trattamentale svolta:

In relazione all'attività trattamentale sopradescritta sono state implementate le seguenti misure di sicurezza tecniche:

Descrivere esclusivamente le misure adottate per la presente attività trattamentale

Crittografia:

Tecniche di Anonimizzazione:

Tecniche di Pseudonimizzazione:

Partizionamento:

Controllo degli accessi logici:

Tracciabilità:

Sicurezza dell'archiviazione digitale dei documenti:

Lotta contro i malware:

Sicurezza delle piattaforme e/o dei siti web utilizzati:

Backup:

Sicurezza dei canali informatici:

Altra misura di sicurezza tecnica predisposta:

In relazione all'attività trattamentale sopradescritta sono state implementate le seguenti misure di sicurezza organizzative:

Descrivere esclusivamente le misure adottate per la presente attività trattamentale

Sicurezza dell'archiviazione della documentazione cartacea:

Controllo degli accessi fisici:

Prevenzione e protezione dalle fonti di rischio umane:

Prevenzione e protezione dalle fonti di rischio non umane:

Gestione postazioni:

Altra misura di sicurezza fisica e/o organizzativa: