DPIA
ex art. 35 GDPR

Sommario

IL CONTESTO NORMATIVO DEL DATA PROTECTION IMPACT ASSESSMENT 3
Data Protection Impact Assessment 9
CONTESTO 9
B) MISURE DI SICUREZZA 13
B.1) MISURE DI SICUREZZA ORGANIZZATIVE 13
B.2) MISURE DI SICUREZZA TECNICHE 14
C) DPIA 16
C.1) ACCESSO ILLEGITTIMO 17
C.2) MODIFICA INDESIDERATA 19
C.3) PERDITA ACCIDENTALE 20
GRAFICO DPIA 21

IL CONTESTO NORMATIVO DEL 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 trattamentali. 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. Muovendo i passi dal dettato normativo, segue il testo dell'art. 35 GDPR:

"ART. 35

Valutazione d'impatto sulla protezione dei dati

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."

La disciplina sul *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 i 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 in 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.

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, gli eventi potenzialmente dannosi e suggerire 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 ss.mm.ii.) 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.

In conclusione, il rischio 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).

I principali impatti sui diritti e le libertà degli interessati, qualora il rischio di accesso illegittimo, modifica indesiderata e/o perdita di dati dovesse concretizzarsi, sono rappresentati da:

- perdita del controllo dei dati personali;

- limitazione dei diritti;
- discriminazione;
- furto o usurpazione d'identità;
- frodi;
- perdite finanziarie;
- decifratura non autorizzata alla pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- conoscenza da parte di terzi non autorizzati;
- qualsiasi altro danno economico o sociale significativo;
- danni fisici o psicologici.

Le principali minacce che potrebbero concretizzare il rischio di accesso illegittimo, modifica indesiderata e/o perdita dei dati personali consistono in:

- danni fisici, ossia azioni offensive finalizzate a distruggere, esporre, alterare, disabilitare, sottrarre o ottenere l'accesso non autorizzato a risorse fisiche come l'infrastruttura, l'hardware o l'interconnessione. Rientrano in questa categoria atti di vandalismo, furto, sabotaggio, perdita di informazioni e attacchi massivi riguardanti qualsiasi tipo di infrastruttura, anche quella Internet;
- eventi naturali, ossia eventi che possono distruggere, danneggiare o rendere irrecuperabili risorse fisiche come l'infrastruttura, l'hardware o l'interconnessione (ad esempio fenomeni climatici, incendi, allagamenti, ecc.);
- perdita di servizi essenziali, ossia interruzioni, perdite o malfunzionamenti dei servizi accessori fondamentali per il corretto funzionamento dell'infrastruttura hardware o di interconnessione alle reti informatiche e dati (ad esempio interruzioni nei collegamenti di rete, blackout);

- disturbi, ossia disturbi elettromagnetici o di contorno che possono causare interruzioni o malfunzionamenti dell'infrastruttura hardware o di interconnessione (ad esempio disturbi di rete di tipo intermittente o continuo);
- compromissione di informazioni, ossia azioni mirate ad ascoltare, interrompere o prendere il controllo di una comunicazione di terzi senza il consenso. Le minacce 'legali' comprendono la violazione di norme e leggi, nonché il mancato rispetto dei requisiti contrattuali da parte di prestatori di servizi verso gli utilizzatori dell'infrastruttura di rete (ad esempio furto di documenti o di supporti di memorizzazione);
- problemi tecnici, definiti come guasto o malfunzionamento. Ne sono esempi guasti o interruzioni di dispositivi di rete o sistemi, bug di software o errori di configurazione. Le 'interruzioni' sono disordini inattesi del servizio o riduzione della qualità che scendono al di sotto di un livello richiesto (ad esempio problemi ai software, uso dei servizi da parte di persone non autorizzate);
- azioni non autorizzate, ossia azioni che mirano ai sistemi, alle infrastrutture e/o alle reti mediante azioni dannose. Le minacce comuni sono generalmente definite come attacchi informatici e azioni correlate (ad es. spam, malware, spyware, botnet, manipolazione di hardware e software, alterazioni delle configurazioni, DDoS, sfruttamento di bug dei software, violazione di dati, furto di identità);
- compromissione di funzioni, ossia un danno involontario o accidentale che si riferisce a distruzione, danni fisici e perdite di informazioni per lo più dovuti ad alterazioni del sistema o all'utilizzo inadeguato dei sistemi;
- attacchi di ingegneria sociale, ossia danni veicolati attraverso una serie di tecniche basate su processi cognitivi di influenzamento, inganno e manipolazione che, sfruttando l'ingenua disponibilità e buona fede, nonché l'ignoranza e poca attenzione della vittima, sono finalizzate all'ottenimento di informazioni riservate o sensibili (ad esempio attacchi phishing, divulgazione involontaria delle informazioni).

Data Protection Impact Assessment (DPIA)

Titolare del trattamento: *Istituti Fisioterapici Ospitalieri*

Nome Attività: *Studio di ricerca scientifica" Sedi di recidiva macroscopica in pazienti con recidiva biochimica dopo radioterapia di salvataggio"*

Data di creazione: *10 dicembre 2024*

CONTESTO

Il presente studio di ricerca scientifica è uno studio retrospettivo monocentrico osservazionale.

Obiettivo primario dello studio consiste nel validare, in una casistica di pazienti con recidiva biochimica dopo terapia di salvataggio e rispondenti ai criteri di inclusione previsti, le sedi di recidiva macroscopica dopo terapia di salvataggio, la dose da esse ricevute, i fattori di rischio associati alla comparsa di recidive dopo il suddetto trattamento.

I dati verranno raccolti in un foglio excel appositamente sviluppato per lo Studio dal Promotore. Il file excel, una volta compilato e riempito con i dati

pseudonimizzati dei pazienti arruolati nello Studio, verrà poi protetto da password dal Promotore.

In particolare, per ciascun paziente saranno raccolti ed elaborati i dati provenienti dalla documentazione clinica/cartella clinica e dalle cartelle cliniche e ambulatoriali.

Ad ogni partecipante sarà assegnato un codice identificativo univoco ed esclusivamente il personale autorizzato sarà in grado di risalire all'identità dei soggetti arruolati. I dati pseudonimizzati saranno inseriti in un'apposita scheda raccolta dati/file excel, che sarà accessibile al solo personale autorizzato.

1) Finalità del trattamento:

- ✓ Studio e ricerca scientifica

2) Categorie di interessati:

- ✓ Pazienti

3) Numero di interessati:

- ✓ Da 1 a 100

4) Sono somministrate le informazioni privacy all'interessato?

- ✓ Si

5) Come sono rese all'interessato le informazioni privacy?

- ✓ Trattandosi di uno retrospettivo che prevede la raccolta ed elaborazione di dati riguardanti gli aspetti clinici e patologici precedentemente registrati a scopo clinico o per l'esecuzione di precedenti progetti di ricerca, l'utilizzo e l'elaborazione degli stessi per finalità di ricerca scientifica potrà avvenire in assenza di acquisizione del consenso da parte degli interessati, poiché, nel caso specifico, lo studio è effettuato in base a disposizioni di legge o di regolamento ovvero al diritto dell'Unione europea: art. 110, co.1, art. 110 bis, co.4 Codice Privacy

6) Come si ottiene il consenso degli interessati?

- ✓ Laddove possibile, è prevista la raccolta del consenso al trattamento dei dati personali; ove non possibile, trattandosi di uno studio retrospettivo di dati precedentemente raccolti, l'utilizzo e l'elaborazione degli stessi per finalità di ricerca scientifica può avvenire in assenza di acquisizione del consenso da parte degli interessati, poiché lo studio è effettuato in base a disposizioni di legge o di regolamento ovvero al diritto dell'Unione europea (art. 110, co. 1, art. 110 bis, co.4 Codice Privacy)

7) Sono previste modalità per l'esercizio dei diritti dell'interessato? (quali, il diritto di accesso, di rettifica, di cancellazione, di limitazione, di portabilità dei dati, di opposizione)

- ✓ Si, tramite apposita comunicazione al Promotore (IFO-IRE)

8) Quali sono le modalità per l'esercizio dei diritti dell'interessato?

- ✓ A mezzo mail/PEC
- ✓ A mezzo raccomandata A/R

9) Categorie di dati personali:

- ✓ Dati anagrafici in chiaro
- ✓ Dati anagrafici pseudonimizzati
- ✓ Dati di identificazione elettronica
- ✓ Dati relativi alla salute/sanitari
- ✓ Dati relativi ad immagini diagnostiche

10) Elencare le attività di trattamento effettuate:

- ✓ Raccolta diretta dall'interessato
- ✓ Registrazione
- ✓ Conservazione
- ✓ Organizzazione
- ✓ Consultazione
- ✓ Selezione
- ✓ Estrazione
- ✓ Elaborazione

- ✓ Utilizzo
- ✓ Blocco/Limitazione
- ✓ Comunicazione
- ✓ Cancellazione
- ✓ Distruzione

11) Modalità di conservazione:

- ✓ Digitale
- ✓ Cartacea

12) *Data retention*:

- ✓ Sino al raggiungimento della finalità

13) Categorie di destinatari:

- ✓ Soggetti nominati Responsabili del trattamento ex art. 28 GDPR - Dott.ssa Diana Giannarelli presso il Dipartimento di Statistica della Fondazione Policlinico Universitario A. Gemelli IRCCS
- ✓ Persone Autorizzate per designazione al trattamento ex art. 29 GDPR e 2-quaterdecies Codice Privacy

14) Piattaforme, dispositivi e/o applicativi utilizzati nell'ambito dell'attività di trattamento in esame:

- ➢ *file excel,* conservato in *cloud* istituzionale, appositamente sviluppato per lo studio e protetto da *password;*
- ➢ piattaforma Varian;
- ➢ piattaforma SpeedRo

15) Avviene un trasferimento di dati personali al di fuori dei confini nazionali?

- ✓ No

22) Base giuridica del Trattamento *ex* art. 6 GDPR:

- ✓ Per i pazienti in vita o rintracciabili: consenso dell'interessato (art. 6, par. 1, lett. a) GDPR
- ✓ Per i pazienti deceduti o non rintracciabili: art. 110, art. 110 bis, c. 4 Codice Privacy

23) Base giuridica del trattamento *ex* art. 9 GDPR

- ✓ Per i pazienti in vita o rintracciabili: consenso rafforzato dell'interessato (art. 9, par. 2, lett. a)
- ✓ Per i pazienti deceduti o non rintracciabili: art. 110, art. 110 bis, c. 4 Codice Privacy, art. 9, par. 2, lett. J) GDPR

24) Tipologia di trattamento:

- ✓ Trattamenti non occasionali di dati relativi a soggetti vulnerabili quali minori, disabili, anziani, infermi di mente, pazienti e richiedenti asilo

B) MISURE DI SICUREZZA

B.1) MISURE DI SICUREZZA ORGANIZZATIVE

25) Sicurezza dell'archiviazione della documentazione cartacea:

- ✓ Armadiature con chiave
- ✓ Archivio in stanza/locale dedicato

26) Nomina delle Persone autorizzate per designazione

- ✓ Si

27) Nomina dei delegati al trattamento:

- ✓ Si

28) Nomina dei Responsabili del trattamento:

- ✓ Si

29) Elaborazione ed adozione di policy privacy aziendali:

- ✓ Si

30) Quali?

- ➢ Policy ritiro dei referti online; policy informazioni privacy; policy password; policy chiavi

31) Controllo degli accessi fisici:

- ✓ Si

32) Quali?

- ➢ Accesso all'archivio cartaceo consentito esclusivamente al personale autorizzato

33) Formazione del personale:

- ✓ Si

34) Altra misura di sicurezza fisica e/o organizzativa implementata:

- ➢ Nessuna

B.2) MISURE DI SICUREZZA TECNICHE

35) Crittografia *Database*:

- ✓ File excel: Non applicabile
- ✓ Varian: Non applicabile
- ✓ SpeedRO: Non applicabile

36) Sistema operativo *workstation*:

- ✓ File excel: Windows
- ✓ Varian: Windows
- ✓ SpeedRO: Windows

37) Aggiornamento sistema operativo:

- ✓ File excel: Si
- ✓ Varian: Si
- ✓ SpeedRO: Si

38) Configurazione *workstation*:

- ✓ File excel: Utente con restrizioni
- ✓ Varian: Utente con restrizioni
- ✓ SpeedRO: Utente con restrizioni

39) Tecniche di anonimizzazione:

- ✓ File excel: Non applicabile
- ✓ Varian: Non applicabile
- ✓ SpeedRO: cifratura dati sensibili su unica base dati MPI

40) Tecniche di pseudonimizzazione:

- ✓ File excel: Si (ad ogni partecipante sarà assegnato un codice identificativo univoco con acronimo dello studio ed esclusivamente il personale autorizzato sarà in grado di risalire all'identità dei soggetti arruolati)
- ✓ Varian: codice univoco con acronimo dello studio di riferimento
- ✓ SpeedRO: memorizzazione del solo identificativo MPI

41) Partizionamento:

- ✓ File excel: Si (livello LAN: 802.1q L2 Vlan)
- ✓ Varian: livello LAN: 802.1q L2 Vlan
- ✓ SpeedRO: livello LAN: 802.1q L2 Vlan

42) Controllo degli accessi logici:

- ✓ File excel: Si
- ✓ Varian: Si
- ✓ SpeedRO: Si

43) Quali strumenti vengono utilizzati?

- ✓ File excel: Accesso al *file excel* mediante indirizzo ID e *password*
- ✓ Varian: Non applicabile
- ✓ SpeedRO: Non applicabile

44) Tracciabilità:

- ✓ File excel: Si
- ✓ Varian: Si
- ✓ SpeedRO: marcatura dell'operatore nelle procedure di modifica dati

45) Quali strumenti vengono utilizzati?

- ✓ File excel: Viene utilizzato il sistema di *Audit Log* di Microsoft 365 per garantire la tracciabilità completa delle attività svolte sui *file* e sui dati
- ✓ Varian: Utilizziamo il sistema di Audit Log di Microsoft 365 per garantire la tracciabilità completa delle attività svolte sui file e sui dati.
- ✓ SpeedRO: documenti memorizzati in formato cifrato, recuperabili solo tramite le interfacce utente dei vari moduli, solo previa autenticazione

46) Misure anti malware:

- ✓ File excel: Microsoft 365 include Microsoft Defender for Office 365, che fornisce protezione avanzata contro i *malware* e minacce informatiche, proteggendo *file* e comunicazioni in *cloud, Endpoint software, Antivirus* perimetrale su internet *gateway*
- ✓ Varian: endpoint software, antivirus perimetrale su internet gateway
- ✓ SpeedRO: endpoint software, antivirus perimetrale su internet gateway

47) Backup:

- ✓ File excel: *Daily* incrementale, *Weekly full* (*online retentation* 30 gg, *offline retentation* 90gg), i dati vengono archiviati e protetti nel *cloud* Microsoft 365, che include funzionalità di *backup* automatico e ridondanza
- ✓ Varian: daily incrementale, weekly full (online retention 30gg, offline retention 90gg)
- ✓ SpeedRO: daily incrementale, weekly full (online retention 30gg, offline retention 90gg)

48) Sicurezza dei canali informatici: (es. HTTPS; *firewall*)

- ✓ File excel: Sistema di autenticazione, *Stateful Inspection Firewall,* Protocollo *HTTPS,* Protocollo *SSL,* VPN; IPSec VPN
- ✓ Varian: HTTPS, SSL VPN, IPSec VPN
- ✓ SpeedRO: HTTPS, SSL VPN, IPSec VPN

49) Altra misura di sicurezza tecnica implementata:

- ✓ File excel: *Disaster Recovery*
- ✓ Varian: *Disaster Recovery*
- ✓ SpeedRO: *Disaster Recovery*

C) DPIA

50) Vengono applicate e/o osservate linee guida, *best practice* di settore, norme UNI/ISO/IEC, codice di condotta, regolamenti aziendali, etc.?

- ✓ No

51) La finalità di trattamento è specifica, esplicita e legittima?

- ✓ **Specifica**: è ben delineata ed individuata nella finalità del Titolare di condurre uno studio monocentrico retrospettivo riguardate pazienti con fallimento biochimico (BF) dopo SRT;
- ✓ **Esplicita**: si, in quanto rappresentata agli interessati per il tramite delle Informazioni privacy *ex* art. 13 GDPR sottoposte all'attenzione di questi mediante consegna diretta, laddove fosse possibile raccogliere il consenso al trattamento dei dati personali, nonché pubblicate sul sito web istituzionale;
- ✓ **Legittima:** in quanto conforme alla normativa privacy, poiché è sorretta da un'idonea base giuridica del trattamento e, nello specifico:
  - per i pazienti in vita o rintracciabili: art. 6, par. 1, lett. a) GDPR, nonché art. 9, par. 2, lett. a) GDPR, in quanto *"l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali"*;
  - per i pazienti deceduti o non rintracciabili: art. 110, art. 110 bis, c.4 Codice Privacy, art. 9, par. 2, lett. J) GDPR;

52) Come viene rispettato il principio di minimizzazione dei dati?

- ✓ Sono trattati esclusivamente i dati necessari al perseguimento della finalità del Titolare, consistente nella volontà di condurre uno studio retrospettivo monocentrico riguardate pazienti con fallimento biochimico (BF) dopo SRT. Difatti, i dati personali oggetto di raccolta risultano fondamentali per l'esecuzione dell'attività trattamentale descritta nel contesto; pertanto, i dati raccolti risultano adeguati, pertinenti e limitati rispetto alla specifica finalità, con la conseguenza che il trattamento è legittimo e proporzionato rispetto alla finalità che il Titolare del trattamento intende perseguire

C.1) ACCESSO ILLEGITTIMO

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

- ✓ Perdita del controllo dei dati personali
- ✓ Decifratura non autorizzata della pseudonimizzazione
- ✓ Discriminazione

- ✓ Perdita di riservatezza dei dati personali protetti da segreto professionale
- ✓ Conoscenza da parte di terzi non autorizzati

54) Quali sono le principali minacce che potrebbero concretizzare il rischio?

- ✓ Danni fisici
- ✓ Compromissione di informazioni
- ✓ Problemi tecnici
- ✓ Azioni non autorizzate
- ✓ Attacchi di ingegneria sociale

55) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

C.2) MODIFICA INDESIDERATA

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

- ✓ Discriminazione
- ✓ Limitazione dei diritti

57) Quali sono le principali minacce che potrebbero concretizzare il rischio?

- ✓ Danni fisici
- ✓ Azioni non autorizzate

58) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

C.3) PERDITA ACCIDENTALE

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

- ✓ Limitazione dei diritti
- ✓ Discriminazione

60) Quali sono le principali minacce che potrebbero concretizzare il rischio?

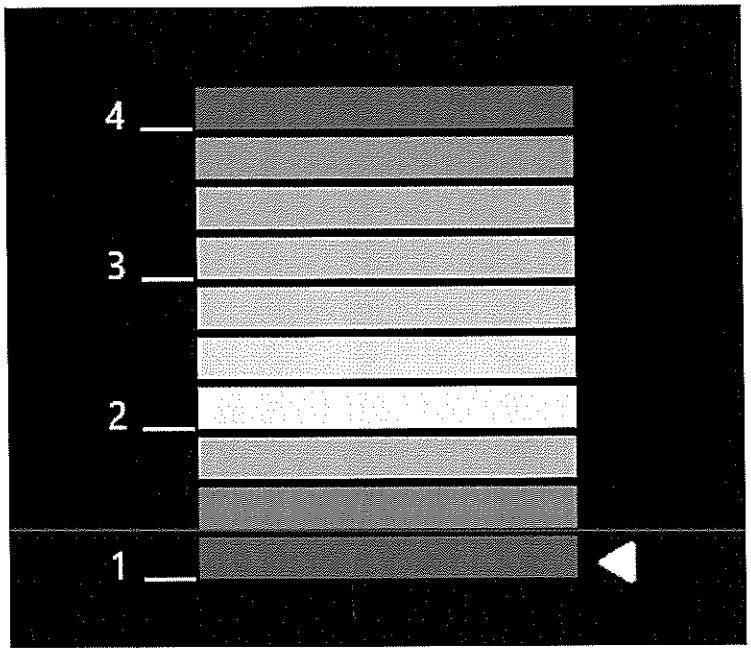
- ✓ Danni fisici
- ✓ Eventi naturali
- ✓ Perdita di servizi essenziali
- ✓ Azioni non autorizzate
- ✓ Compromissione di funzioni

61) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne
- ✓ Fonti non umane

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

GRAFICO DPIA



TRASCURABILE
LIMITATO
SIGNIFICATIVO
MASSIMO

IFO - ISTITUTO REGINA ELENA
DIRETTORE RADIOTERAPIA
Prof. Giuseppe Sanguineti

Firmato digitalmente da:
Gennaro Ciliberto
Data: 20/12/2024 14:32:04