Azienda di Servizi alla Persona
"GOLGI - REDAELLI"

Valutazione d'impatto sulla protezione dei dati - DPIA

Attività di trattamento **Prestazioni legate a servizi riabilitativi dell'età evolutiva**
Soggetti interessati Soggetti minori affetti da disturbi del comportamento e dello spettro autistico; parenti, familiari, care givers, amministratori di sostegno, curatori, tutori.

Responsabile elaborazione DPIA:	Titolare del trattamento	**Posizione:**	Direttore Generale- Rappresentante Legale

Redatta in collaborazione con il Responsabile della Protezione dei Dati

Sommario

Nozione di valutazione d'impatto

Il Data Protection Impact Assessment (DPIA) è un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. Si tratta di una valutazione preliminare eseguita dal Titolare del trattamento dei dati relativamente agli impatti di un trattamento laddove dovessero essere violate le misure di protezione.
Il DPIA va inquadrato come uno strumento essenziale e fondamentale al fine di dar corso al nuovo approccio alla protezione dei dati personali richiamato dal regolamento europeo e fortemente basato sul principio della accountability.

Quadro normativo

- REGOLAMENTO 2016/679/UE: Articoli 35 e 36
- D. Lgs. 196/2003 smi
- Considerando C84, C89, C90, C91, C92, C93, C94, C95
- WP248 - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679
- provvedimento Garante n. 467 dell'11.10.2018 – G.U. 269 del 19.11.2018

Motivi della valutazione d'impatto

L'attività di trattamento oggetto della presente valutazione d'impatto – DPIA considerati la natura, l'oggetto, il contesto e le finalità del trattamento, potrebbe presentare un rischio elevato per i diritti e le libertà delle persone fisiche secondo i criteri di cui all'art.35, c. 3 del GDPR 2016/679.
Il trattamento ricade nelle seguenti due categorie per le quali si rende necessario lo sviluppo di un processo di valutazione di impatto in base alle indicazioni della linea guida WP248:

- dati sensibili o dati aventi carattere altamente personale
- dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati può causare squilibrio di potere tra il titolare del trattamento e gli interessati, che potrebbero non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti.

E' inoltre compresa nell'elenco di trattamenti soggetti al requisito di una valutazione d'impatto redatto dall'Autorità di controllo nazionale (Garante per la Privacy – provvedimento 467/18 - allegato 1- punto 6. "Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)).

Metodo di conduzione della DPIA

Scopo dell'attività è quella di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento è conforme al regolamento GDPR e in seconda battuta comprendere se quel trattamento deve essere sottoposto ad una valutazione DPIA.
Il presente documento comprende, principalmente:

- una descrizione sistematica del trattamento previsto e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità del trattamento in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati.

Nello svolgimento della DPIA, il titolare del trattamento ha provveduto a raccogliere le opinioni dei rappresentanti degli interessati, non titolati ad agire in prima persona a motivo della minore età. Il dato è stato raccolto a cura della struttura di riferimento mediante somministrazione di questionario - precedentemente condiviso con il RPD, ed allegato al presente documento - in forma anonima nel periodo 12.01/01.03.2019, ed ha avuto come riscontro la restituzione di 33 questionari.
L'esame delle risposte ai quesiti posti ha permesso di rilevare che per la totalità del campione coinvolto le attività di trattamento dei dati poste in essere dall'ASP Golgi-Redaelli:
- sono lecite e rispettose dei principi di correttezza e trasparenza
- prevedono misure di protezione dei dati idonee ad attenuare i rischi per i diritti e le libertà delle persone fisiche interessate al trattamento.

Solo in due casi, invece, non è stata data risposta al quesito circa
- l'effettiva necessità e proporzionalità del trattamento in relazione alle finalità perseguite,

che per i restanti 31 casi ha avuto risposta affermativa.

In ossequio al principio del *data protection by design* il Titolare del Trattamento ha consultato il Responsabile della Protezione dei Dati circa:

- se condurre o meno la presente DPIA
- se condurre la DPIA con risorse interne o esternalizzandola
- quale metodologia adottare per la conduzione della stessa
- quali salvaguardie applicare per attenuare i rischi per i diritti e gli interessi delle persone interessate

Il Responsabile della Protezione dei Dati si è espresso favorevolmente sulla correttezza della conduzione della DPIA e sulla conformità alle normative vigenti delle conclusioni raggiunte, dato altresì atto che la decisione finale del titolare del trattamento non si discosta dalle opinioni degli interessati appositamente interpellati.

Valutazione preliminare

FASE 1 - Descrizione del trattamento

Soggetti interessati

Soggetti minori affetti da disturbi del comportamento e dello spettro autistico; parenti, familiari, care givers, amministratori di sostegno, curatori, tutori.

Finalità del trattamento

- Erogazione degli interventi riabilitativi. Attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal SSN e di assistenza domiciliare; interventi anche di rilievo sanitario in favore di soggetti non autosufficienti o incapaci, ivi compresi i servizi di assistenza domiciliare, accompagnamento e trasporto; attività correlate all'applicazione della disciplina in materia di assistenza, integrazione sociale e diritti delle persone; programmazione, gestione, controllo e valutazione dell'assistenza sanitaria; instaurazione, gestione e controllo tra l'amministrazione e i soggetti accreditati o convenzionati del SSN; scopi di ricerca scientifica; attività svolte dagli Uffici relazioni con il Pubblico.
- Esercizio del diritto alla difesa in sede amministrativa e/o giudiziaria; attività dirette all'accertamento della responsabilità civile, disciplinare e contabile – esame dei ricorsi amministrativi – comparire in giudizio o partecipare alle procedure conciliative nei casi previsti dalla legge o dai CCNL; attività degli URP; attività di gestione dei rapporti assicurativi con riferimento a sinistri, danni, responsabilità verso terzi etc.; attività di recupero delle posizioni debitorie nei confronti dell'Azienda.
- Scopi storici concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi storici degli enti pubblici; gestione degli archivi di deposito per conto delle Aree/Direzioni/Servizi competenti mediante conservazione dei fascicoli di rispettivo interesse; pubblicazioni di carattere storico e scientifico; comunicazioni diverse relative all'attività aziendale, a livello divulgativo, promozionale o statistico.
- Sicurezza e protezione di persone e beni; svolgimento di attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal SSN.
- Esecuzione di compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Descrizione del trattamento e flussi informativi

Il trattamento viene posto in essere allo scopo di fornire interventi di logopedia (per disturbi specifici del linguaggio e dell'apprendimento), di psicomotricità (per i disturbi relazionali e comportamentali e per deficit cognitivi), di riabilitazione neurovisiva e di riabilitazione neuromotoria, interventi di psicoterapia per l'età evolutiva con possibilità di colloqui con i genitori.

In particolare, per i soggetti ai quali l'Azienda presta servizi, i dati vengono trattati ai fini di:

- riabilitazione
- programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
- attività certificatorie
- applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione
- instaurazione, gestione, pianificazione e controllo dei rapporti con la Regione Lombardia, le Aziende Sanitarie Locali e le Aziende Ospedaliere, nonché con altri soggetti accreditati o convenzionati del Servizio Sanitario Nazionale e Regionale
- instaurazione e gestione del rapporto contrattuale sotteso alla erogazione dei servizi e delle prestazioni e dei rapporti con altri enti e soggetti pubblici e privati
- adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione.

I dati vengono forniti, mediante presentazione di apposita istanza o di idonea prescrizione, dai soggetti che esercitano nei confronti dell'interessato la patria potestà, o rivestono la qualifica di tutori o da terzi (pediatra di riferimento, medico di base, medico delle UONPIA o dei servizi territoriali, ASL, Comune, Autorità diverse, etc.) e possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente. I dati sensibili relativi allo stato di salute vengono trattati per la gestione delle situazioni patologiche e per l'erogazione delle prestazioni socio-sanitarie agli interessati, nell'ambito delle finalità istituzionali dell'Azienda e in ottemperanza alla normativa regionale in materia. I dati e le operazioni correlate ad eventuali attività di ricerca, specificati nei singoli progetti, qualora non sia possibile l'utilizzo di dati anonimi, sono trattati comunque in modo da non poter identificare gli interessati, a meno che l'abbinamento di tali dati identificativi al materiale di ricerca non sia temporaneo e essenziale per il risultato della ricerca, e motivato per iscritto nel progetto di ricerca.

Al fine di instaurare e gestire le procedure connesse alle prestazioni erogate, in molti casi è necessario ed indispensabile anche il trattamento di dati dei familiari o care givers dell'utente diretto.
I dati sono oggetto di trattamento presso le strutture organizzative competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando.
Le informazioni relative alle prestazioni erogate sono strutturate in cartelle cliniche e/o fascicoli sociosanitari ai sensi delle vigenti disposizioni regionali in materia.
Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia.
I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.

Dati oggetto del trattamento

Dati relativi a: Origine razziale ed etnica; Convinzioni religiose, filosofiche, di altro genere; Stato di salute: attuale, pregresso, relativo a familiari dell'interessato.

Modalita' di trattamento

Con ausilio di strumenti elettronici / Senza ausilio di strumenti elettronici

Operazioni eseguite

Raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione.

Conservazione dei dati trattati

I dati sono conservati in archivi elettronici e/o in archivi cartacei.

Processi aziendali coinvolti nel trattamento

Le principali strutture coinvolte a diverso titolo nel trattamento dei soli dati necessari allo svolgimento delle rispettive competenze sono: istituto Golgi; servizio accreditamenti sociosanitari; area pianificazione, controllo di gestione e sistemi informativi; area contabilità, rendicontazione e fatturazione; area giuridico-legale.

FASE 2 - Valutazione della conformita'

Modalita' di raccolta dei dati

Raccolta diretta presso l'interessato (i dati vengono forniti dai soggetti che esercitano nei confronti dell'interessato la patria potestà, o rivestono la qualifica di tutori) /da soggetti terzi (pediatra di riferimento, medico di base, medico delle UONPIA o dei servizi territoriali, ASL, Comune, Autorità diverse, etc.).

Soggetti che hanno accesso ai dati

Titolare del trattamento. Responsabili del trattamento e incaricati del trattamento riferiti alle diverse strutture aziendali interessate per competenza. Responsabili esterni del trattamento come individuati dall'Azienda in ragione degli incarichi conferiti/dei servizi affidati.
E' consentita la comunicazione dei dati ad altri soggetti pubblici e privati in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali - con riferimento alle diverse tipologie di soggetti interessati e ai rispettivi rapporti intercorrenti con l'Azienda – in particolare come segue:
- *Unità Neuropsichiatriche Infantili di Base; *servizi scolastici; *servizi sociali; *servizi sanitari (neuropsichiatria infantile ospedaliera, pediatri di base, altri specialisti); *altre figure professionali dell'ambito pediatrico, per comunicazioni relative a relazioni cliniche diagnostiche, valutazioni, diagnosi funzionali, piani riabilitativi, esiti di gruppi operativi
- *soggetti controinteressati nell'istruttoria dei ricorsi amministrativi; *consulenti tecnici incaricati dall'Autorità Giudiziaria, collegi di conciliazione presso la Direzione provinciale del lavoro; *Autorità Giudiziaria; *Forze di Polizia; *Società assicuratrici (per la valutazione e copertura economica degli indennizzi per la responsabilità civile verso terzi); *incaricati di indagini difensive proprie e altrui, società di recupero crediti; *consulenti della controparte; *eventuali Amministrazioni coinvolte
*altri soggetti pubblici (in particolare, *Autorità giudiziaria e di P.S. dietro specifica richiesta).

Modalita'di trasferimento dei dati a soggetti terzi

In formato elettronico o cartaceo.

Modalita' di aggiornamento e eliminazione dei dati

E' previsto l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza da parte dei soggetti responsabili del trattamento, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi.
I dati informatici non più occorrenti vengono di norma cancellati o distrutti (anche facendone richiesta all'Amministratore di Sistema, ove il soggetto responsabile non fosse in possesso delle necessarie abilitazioni); qualora fossero conservati, non sono comunque utilizzabili.

I documenti cartacei riportanti dati non più occorrenti - se non protocollati e/o allegati in fascicolo - vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili.
I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di un eventuale riutilizzo; se ciò non è possibile devono essere distrutti.

Motivazione legittima per il trattamento (anche per categorie speciali di dati)/base giuridica del trattamento

Consenso; obblighi legali cui è soggetto il titolare del trattamento; norme di legge o, nei casi previsti dalla legge, di regolamento.

Modalità di offerta di informativa agli interessati e di raccolta del consenso

Su modulistica predisposta a livello aziendale: precedentemente alla raccolta dei dati; direttamente all'atto della richiesta della prestazione. Modulistica disponibile anche via web.

Utilizzo per nuove/diverse finalità di dati personali già raccolti

Non è previsto

Modalità di verifica della accuratezza dei dati personali raccolti e trattati

Verifiche documentali; approfondimenti presso i soggetti rilascianti, nel caso di dati raccolti presso altri soggetti (es.: pediatra di riferimento, medico di base, medico delle UONPIA o dei servizi territoriali, ASL, Comune, Autorità diverse,….).

Asset model a sostegno dei trattamenti

Hardware, software, archivi, reti e piattaforme aziendali.

Periodo massimo di conservazione dei dati

I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.

Misure di sicurezza a garanzia della riservatezza dei dati / per prevenire trattamenti di dati personali non autorizzati o illegittimi

organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative
fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti
logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione
Per il dettaglio si rimanda al Registro del trattamento dei dati, artt. 5 e 6.

Trasferimento di dati personali in un paese non facente parte dell'unione europea

Non è previsto

Diritti degli interessati

L'interessato ha diritto di chiedere al titolare del trattamento l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento; può inoltre opporsi al trattamento ed esercitare il diritto alla portabilità dei dati forniti e trattati in via automatizzata, con il consenso dell'interessato o sulla base di contratto stipulato fra le parti. I diritti riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
È diritto dell'interessato proporre reclamo avverso il trattamento dei dati operato dall'Azienda alla competente Autorità di Controllo (Garante per la protezione dei dati personali), ovvero ricorso dinanzi all'Autorità Giudiziaria.

Il trattamento rispetta

- i principi di liceità, correttezza e trasparenza
- il principio di limitazione della finalità
- il principio di minimizzazione dei dati
- il principio di esattezza dei dati
- il principio di limitazione della conservazione dei dati
- il diritto di informazione
- il diritto di accesso ai dati
- il diritto di portabilità
- il diritto di rettifica
- il diritto di cancellazione (diritto all'oblio)
- il diritto di limitazione del trattamento
- il diritto di opposizione al trattamento

FASE 3 - CONDURRE LA DPIA?

Le risultanze della valutazione preliminare dianzi condotta non paiono evidenziare la sussistenza di rischi aventi particolare impatto su diritti e libertà delle persone i cui dati sono oggetto di trattamento. Peraltro, il trattamento in esame risulta essere posto in essere già precedentemente all'entrata in vigore del Regolamento UE, sin dall'adozione da parte

dello Stato italiano del Codice della Privacy, e da allora condotto sulla base dello stretto rispetto delle norme di riferimento in materia vigenti nel tempo (del resto, in gran parte coerenti con le nuove disposizioni europee), senza che si siano rilevati eventi dannosi nel periodo. Alla luce di tali considerazioni, si ritiene che eventuali rischi possano ritenersi sostanzialmente nel complesso **accettabili.**
In ogni caso, seppure il trattamento di cui si tratta non preveda neppure l'uso di nuove tecnologie, l'Azienda - anche in considerazione della rilevante delicatezza dei dati trattati - ritiene comunque utile la conduzione di attività di miglior approfondimento della valutazione in questione.

Quindi, la tabella seguente illustra i principali rischi afferenti alla protezione dei dati, che si ritengono identificabili in fase di valutazione preliminare, correlati ad eventi relativi al contesto in cui si opera o relativi agli strumenti, oppure a comportamenti degli operatori:

Descrizione del rischio
Danneggiamento/ perdita/distruzione non autorizzata dati personali
Accesso non autorizzato dati personali
Trattamento non autorizzato (comprensivo di modifica, divulgazione……)
Trattamento non conforme alla finalità della raccolta o illecito

Esecuzione DPIA

Fase 1 - Informazioni integrative per analisi del rischio

(in aggiunta a quanto già esposto in sede di valutazione preliminare, cui si rimanda)

Tecnologie utilizzate

Non 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

Metodi di identificazione

Non verranno utilizzati nuovi metodi di identificazione dei dati, ma verranno riutilizzati identificatori già esistenti ed in uso.
Non verranno utilizzati nuovi o significativamente modificati requisiti di autentica di identità, che possono risultare intrusivi od onerosi

Coinvolgimento di altre strutture

L'iniziativa di trattamento coinvolge altre strutture, sia pubbliche, sia private, sia appartenenti a settori non-profit e volontari

Modifiche alle modalità di trattamento dei dati

L'iniziativa di trattamento non apporterà nuove o significative modifiche alle modalità di trattamento dei dati personali, che potrebbero destare preoccupazioni nell'interessato.
I dati personali, afferenti all'interessato, già presenti in un esistente data base, non verranno assoggettati a nuove o modificate modalità di trattamento.
L'iniziativa di trattamento non apporterà nuove o significative modifiche alle modalità di consolidamento, interscambio, riferimenti incrociati, abbinamento di dati personali, provenienti da più sistemi di trattamento.

Modifiche alle procedure di trattamento dei dati

Il trattamento non potrà introdurre nuove modalità e procedure di raccolta dei dati, che non siano sufficientemente trasparenti o siano intrusive, né modifiche a sistemi e processi, appoggiati a normative in vigore, che possano avere esiti non chiari o non soddisfacenti, o che modifichino il livello di sicurezza dei dati, in modo da portare ad esiti non chiari o non soddisfacenti.
Il trattamento non potrà introdurre nuove o modificate procedure sicure di accesso ai dati o modalità di comunicazione e consultazione, che possano essere non chiare o permissive.
Il trattamento non introdurrà nuove o modificate modalità di conservazione dei dati, che possano essere non chiare o prolungate oltremodo.

Esenzioni dalla applicazione delle disposizioni del regolamento

L'attività di trattamento non esula dall'ambito delle disposizioni legislative dell'unione europea, non è svolto da una persona fisica esclusivamente per fini personali e familiari e non è svolta da autorità pubbliche al fine di prevenzione, indagine, individuazione e perseguimento di reati o al fine di applicare pene.

Fase 2 - Valutazione del rischio

a) metodologia di valutazione

L'analisi del rischio è un processo per identificare e valutare il danno causabile da minacce e vulnerabilità in combinazione su uno o più asset aziendali ben precisi. Serve inoltre a giustificare le contromisure, a valutare che siano efficaci, di costo ragionevole, effettivamente applicabili al contesto e in grado di rispondere in tempo alle minacce. Tale

analisi ha come obiettivo minimizzare la probabilità di accadimento dei rischi e gli impatti che possibili violazioni dei dati personali potrebbero comportare agli individui, come di seguito esemplificativamente sintetizzati:
Rischi: distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato ai dati personali.
Impatto:

- da violazione della sicurezza fisica
- da violazione dei dati di identificazione o attinenti l'identità personale
- materiale (perdite finanziarie o al patrimonio)
- morale o biologico (turbamento per la diffusione di una notizia riservata, compromissione di uno stato salute, evento lesivo di diritti umani o integrità della persona)
- sociale (conseguenze di tipo discriminatorio, perdite di autonomia)

La DPIA si basa su un'analisi dei rischi centrata su
- rischi derivanti da contenuto intrinseco del trattamento
- rischi derivanti da possibili violazioni di sicurezza
in relazione ai possibili controlli applicabili, ricavando, così, un **indice di rischio "normalizzato"** rispetto al contesto aziendale.

Il rischio normalizzato RN viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, V)

dove:

P = probabilità (stima della probabilità di accadimento degli eventi che causano la perdita, violazione, distribuzione non controllata di dati = **pericoli**)

C = conseguenze generate dall'evento (stima della gravità dei danni attesi rispetto all'accadimento di un determinato evento)

V = vulnerabilità rispetto al grado di adeguatezza delle misure (grado di adeguatezza delle misure che contrastano il manifestarsi degli eventi)

In prima battuta viene ricavato il **rischio intrinseco Ri** come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla probabilità P è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITÀ	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle conseguenze C è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

La **matrice** che scaturisce dalla combinazione di probabilità e conseguenze è rappresentata in figura seguente:

PROBABILITA'	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8

	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	(1 ≤ Ri ≤ 2)
Basso	(3 ≤ Ri ≤ 4)
Rilevante	(6 ≤ Ri ≤ 9)
Alto	(12 ≤ Ri ≤ 16)

Per ricavare il **Rischio Normalizzato RN**, viene introdotto il fattore Vulnerabilità che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla vulnerabilità V è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		VALORE
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

□ 0,25; □ 0,5; □ 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

VULNERABILITA'	1	1 < RN ≤ 2	3 ≤ RN ≤ 4	6 ≤ RN ≤ 9	12 ≤ RN ≤ 16
	0,5	0,5 < RN ≤ 1	1,5 ≤ RN ≤ 2	3 < RN ≤ 5	6 ≤ RN ≤ 8
	0,25	0,25 ≤ RN ≤ 0,5	0,75 ≤ RN ≤ 1	1,5 ≤ RN < 3	3 ≤ RN ≤ 4
		1 ≤ Ri ≤ 2	3 ≤ Ri ≤ 4	6 ≤ Ri ≤ 9	12 ≤ Ri ≤ 16
		RISCHIO INTRINSECO			

RISCHIO NORMALIZZATO	
RN = Ri x V	Valori di riferimento
Molto basso	0,25 ≤ RN ≤ 1
Basso	1 < RN < 3
Rilevante	3 ≤ RN ≤ 9
Alto	12 ≤ RN ≤ 16

b) definizione di aree di pericolo, rischi generati e valutazione del livello di rischio intrinseco

Di seguito la suddivisione delle principali aree di pericolo con i rischi generati, e le relative stime su probabilità di accadimento e conseguenze:

PERICOLO	RISCHI	PROBABILITA' stimata	CONSEGUENZE stimate
Agenti fisici (incendio, allagamento, attacchi esterni)	• Danneggiamento • Perdita	• Poco probabile	• Gravi

	• Distruzione non autorizzata		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• Danneggiamento • Perdita • Distruzione non autorizzata	• Improbabile	• Gravi
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	• Danneggiamento • Perdita • Distruzione non autorizzata	• Poco probabile	• Limitate
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• Danneggiamento • Perdita • Distruzione non autorizzata • Accesso dati non autorizzato	• Probabile	• Gravi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• Perdita • Distruzione non autorizzata • Accesso dati non autorizzato	• Poco probabile	• Gravi
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• Danneggiamento • Perdita • Distruzione non autorizzata • Accesso dati non autorizzato • Trattamento non autorizzato • Trattamento non conforme alla finalità della raccolta o illecito	• Poco probabile	• Gravi

Rischio intrinseco *(valutato sulla base della media dei valori peggiori di probabilità e conseguenza stimati per rischio specifico)*

• RISCHIO: Danneggiamento / Perdita / Distruzione non autorizzata		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante

• RISCHIO: Accesso non autorizzato		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante

• RISCHIO: Trattamento non autorizzato		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante

• RISCHIO: Trattamento non conforme alla finalità della raccolta o illecito		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante

c) valutazione dell'idoneità delle misure di sicurezza tecniche e organizzative a rendere il rischio accettabile

TRATTAMENTO CON L'AUSILIO DI STRUMENTI ELETTRONICI

Rischio	**Misure**	**Idoneità**
danneggiamento, distruzione o perdita del dato	- effettuazione di copie di sicurezza, salvataggio settimanale dei dati, backup centralizzato periodico, aggiornamento annuale dei programmi di protezione per elaboratore (semestrale per trattamento di dati sensibili o giudiziari) - effettuazione di backup full dei database dei gestionali giornalieri conservando gli ultimi 7 - effettuazione di 2/3/4 snapshot al giorno dei sistemi operativi virtuali presenti sull'infrastruttura principale (Syneto) che consentono un'attivazione in	ADEGUATE

	tempi brevi del servizio eventualmente coinvolto in un malfunzionamento/errore/danno hardware o software. Essi vengono conservati in un NAS appositamente adibito (DS-Syneto) collocato nella sala server secondaria. - effettuazione periodica di restore (dei dati di backup) del database del gestionale principale; - ripristino periodico di snapshot. - dotazione di impianti antincendio - adozione di sistemi di ridondanza sui server - presenza di almeno due alimentatori su ogni server - utilizzo di dischi con RAID e hotspare sui sistemi di produzione - utilizzo di infrastrutture servite da alimentazione privilegiata (gruppo elettrogeno) ed UPS per i sistemi di produzione	
accesso non autorizzato (ai locali, al sistema ed ai dati)	- i server aziendali sono collocati in locali chiusi a chiave (porte blindate o tradizionali), di norma senza finestre e in taluni casi dotati di telecamera IP con registrazione remota - i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persone diverse dalle autorizzate - assegnazione di credenziali di accesso alla rete differenziate per servizio/gestionale e di password personalizzate - adozione di sistema di gestione degli utenti che associa il data base degli stessi con le rispettive autorizzazioni, disponibile centralmente in rete al fine di un eventuale recupero su richiesta dei soggetti autorizzati al trattamento dei dati - utilizzo di salvaschermo protetti da password in caso di inattività - tutti i PC fissi e mobili e gli elaboratori sono coperti da sistemi di rilevamento e di prevenzione delle intrusioni e anti-hackers, firewall di sistema, antivirus, antispyware la cui efficacia è periodicamente verificata ed aggiornata - attivazione di switch e access point di rete in cui sono state configurate VLAN	ADEGUATE
trattamento non autorizzato	- ogni incaricato del trattamento è munito di credenziali di autenticazione e/o parola chiave; è operativa la procedura che ne consente l'autonoma sostituzione periodica da parte del singolo operatore - di norma il codice identificativo personale fornito ad ogni operatore non viene assegnato a persone diverse; - i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persona diversa dall'incaricato del trattamento - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative - implementazione di regole centralizzate finalizzate ad aumentare la robustezza delle password	ADEGUATE

trattamento non conforme alla finalità della raccolta o illecito	- è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, dati non più occorrenti vengono di norma cancellati o distrutti (anche facendone richiesta all'Amministratore di Sistema, ove il soggetto responsabile non fosse in possesso delle necessarie abilitazioni); qualora fossero conservati, non sono comunque utilizzabili.	ADEGUATE

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Rischio	**Misure**	**Idoneità**
accesso non autorizzato	- la conservazione dei documenti contenenti dati personali e/o sensibili avviene in archivi ad accesso selezionato e controllato; i locali in cui sono conservati tali documenti devono essere chiusi al termine dell'orario di lavoro - i documenti contenenti dati sensibili, se affidati all'incaricato del trattamento, devono da questo essere conservati in modo tale da non garantire a terzi la consultabilità degli stessi fino alla restituzione all'archivio d'ufficio - l'accesso agli archivi non è consentito dopo l'orario di chiusura degli stessi, coincidente con l'orario di chiusura degli uffici o con l'effettivo termine delle attività lavorative. Peraltro, qualora si renda necessario consentire l'accesso agli archivi dopo l'orario di chiusura degli stessi, occorre prevedere procedure di controllo e di identificazione e registrazione dei soggetti ammessi, fatte salve preventive autorizzazioni - i documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro - fare attendere soggetti estranei in luoghi in cui non siano presenti informazioni riservate o dati personali; se per ragioni di lavoro gli stessi possono accedere agli uffici, avere cura di riporre eventuali documenti e se necessario di attivare il salvaschermo dei p.c. - evitare l'esportazione di dati personali e/o l'installazione degli stessi su attrezzature diverse da quelle messe a disposizione dall'Azienda (ad es. computer di casa)	ADEGUATE
trattamento non autorizzato	- gli incaricati al trattamento sono autorizzati al trattamento dei soli dati la cui conoscenza sia strettamente necessaria per lo svolgimento dell'incarico affidato o per l'espletamento delle competenze attribuite alla struttura organizzativa di riferimento - divieto di richiedere, raccogliere e/o conservare in fascicolo dati personali non pertinenti con le competenze e le attività svolte o eccedenti le necessità istruttorie delle attività assegnate - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative - il trasporto di dati personali all'esterno dei locali ove si svolge il trattamento, ma comunque all'interno dell'Azienda avviene in modo da garantirne la	ADEGUATE

	riservatezza	
trattamento non conforme alla finalità della raccolta o illecito	- i dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo - è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, i documenti riportanti dati non più occorrenti - se non protocollati e/o allegati in fascicolo - vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili. - i supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di un eventuale riutilizzo; se ciò non è possibile devono essere distrutti	ADEGUATE

d) valutazione rischio normalizzato (sulla base del valore peggiore assegnato alle misure di sicurezza relativamente al rischio specifico).

• RISCHIO: Danneggiamento / Perdita / Distruzione non autorizzata		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	BASSO

• RISCHIO: Accesso non autorizzato		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	BASSO

• RISCHIO: Trattamento non autorizzato		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	BASSO

• RISCHIO: Trattamento non conforme alla finalità della raccolta o illecito		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	BASSO

Risultati DPIA

A valle dell'indagine DPIA condotta l'attività ricade in fascia BASSA.

In **appendice** sono illustrati in sintesi tutti i rischi identificati e le opzioni che permettano di mitigare, evitare o mettere sotto controllo questi stessi rischi, con evidenza del grado di rischio normalizzato.
Si dà inoltre conto della previsione di ulteriori possibili misure di sicurezza tecniche e organizzative atte ad assicurare un ancor maggiore contenimento dei rischi, in via di implementazione o di prossima attuazione.
Si uniscono per completezza di informazione le misure di tutela della privacy nell'esercizio della professione sanitaria e delle attività correlate, adottate allo scopo di prevenire e/o limitare violazioni della riservatezza.

Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati

Secondo le buone prassi, è opportuno che la presente valutazione d'impatto venga riesaminata periodicamente, e particolarmente quando nell'intervallo di tempo trascorso dal completamento della DPIA si siano verificate delle modifiche nei rischi connessi al trattamento o vengano messe in evidenza delle anomalie.
A seguire alcuni esempi di modifiche alle attività di trattamento, rischi connessi e cambiamenti nel contesto organizzativo o sociale che debbono indurre ad una revisione della DPIA:
- Cambiamento sulle attività di trattamento, in termini di:
    - Contesto o finalità del trattamento,
    - Tipologia di dati personali trattati
    - Destinatari o modalità di raccolta dei dati personali
    - Combinazioni di dati provenienti da fonti differenti
    - Trasferimento di dati all'estero
- Modifica ai rischi con impatto sui diritti degli interessati derivati da:
    - Presenza di nuove minacce
    - Modifica ai sistemi informativi a supporto del trattamento
    - Soppressione di contromisure esistenti
    - Nuovi scenari di rischio
    - Nuovi potenziali impatti sulle dimensioni di analisi (Riservatezza, Integrità, Disponibilità)
    - Attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali.

Inoltre, si rende comunque necessaria una revisione della DPIA tutte le volte che si è in presenza di mutamenti nel contesto organizzativo o sociale per il trattamento in essere.

Appendice

1) Tabella dei rischi afferenti alla DPIA

Descrizione del rischio	Rischi inerenti alla protezione dei dati			Opzioni che permettono di evitare o mitigare questo rischio	Rischi residui		
	Probabilità	Conseguenze	Livello di rischio		Probabilità	Conseguenze	Livello di rischio
Danneggiamento/ perdita/distruzione non autorizzata dati personali	Poco probabile	Gravi	Rilevante	- effettuazione di copie di sicurezza, salvataggio settimanale dei dati, backup centralizzato periodico, aggiornamento annuale dei programmi di protezione per elaboratore (semestrale per trattamento di dati sensibili o giudiziari) - effettuazione di backup full dei database dei gestionali giornalieri conservando gli ultimi 7 - effettuazione di 2/3/4 snapshot al giorno dei sistemi operativi virtuali presenti sull'infrastruttura principale (Syneto) che consentono un'attivazione in tempi brevi del servizio eventualmente coinvolto in un malfunzionamento/errore/danno hardware o software. Essi vengono conservati in un NAS appositamente adibito (DS-Syneto) collocato nella sala server secondaria. - effettuazione periodica di restore (dei dati di backup) del database del gestionale principale; - ripristino periodico di snapshot. - dotazione di impianti antincendio - adozione di sistemi di ridondanza sui server - presenza di almeno due alimentatori su ogni server - utilizzo di dischi con RAID e hotspare sui	Poco probabile	Gravi	**BASSO**

				sistemi di produzione - utilizzo di infrastrutture servite da alimentazione privilegiata (gruppo elettrogeno) ed UPS per i sistemi di produzione			
Accesso non autorizzato dati personali	Poco probabile	Gravi	Rilevante	*Trattamento con strumenti elettronici* - i server aziendali sono collocati in locali chiusi a chiave (porte blindate o tradizionali), di norma senza finestre e in taluni casi dotati di telecamera IP con registrazione remota - i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persone diverse dalle autorizzate - assegnazione di credenziali di accesso alla rete differenziate per servizio/gestionale e di password personalizzate - adozione di sistema di gestione degli utenti che associa il data base degli stessi con le rispettive autorizzazioni, disponibile centralmente in rete al fine di un eventuale recupero su richiesta dei soggetti autorizzati al trattamento dei dati - utilizzo di salvaschermo protetti da password in caso di inattività - tutti i PC fissi e mobili e gli elaboratori sono coperti da sistemi di rilevamento e di prevenzione delle intrusioni e anti-hackers, firewall di sistema, antivirus, antispyware la cui efficacia è periodicamente verificata ed aggiornata *Trattamento senza strumenti elettronici* - la conservazione dei documenti contenenti dati personali e/o sensibili avviene in archivi ad accesso selezionato e controllato; i locali in cui sono conservati tali documenti devono essere chiusi al termine dell'orario di lavoro - i documenti contenenti dati sensibili, se affidati all'incaricato del trattamento, devono	Poco probabile	Gravi	**BASSO**

				da questo essere conservati in modo tale da non garantire a terzi la consultabilità degli stessi fino alla restituzione all'archivio d'ufficio - l'accesso agli archivi non è consentito dopo l'orario di chiusura degli stessi, coincidente con l'orario di chiusura degli uffici o con l'effettivo termine delle attività lavorative. Peraltro, qualora si renda necessario consentire l'accesso agli archivi dopo l'orario di chiusura degli stessi, occorre prevedere procedure di controllo e di identificazione e registrazione dei soggetti ammessi, fatte salve preventive autorizzazioni - i documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro - fare attendere soggetti estranei in luoghi in cui non siano presenti informazioni riservate o dati personali; se per ragioni di lavoro gli stessi possono accedere agli uffici, avere cura di riporre eventuali documenti e se necessario di attivare il salvaschermo dei p.c. - evitare l'esportazione di dati personali e/o l'installazione degli stessi su attrezzature diverse da quelle messe a disposizione dall'Azienda (ad es. computer di casa)			
Trattamento non autorizzato (comprensivo di modifica, divulgazione……) dei dati personali	Poco probabile	Gravi	Rilevante	*Trattamento con strumenti elettronici* - ogni incaricato del trattamento è munito di credenziali di autenticazione e/o parola chiave; è operativa la procedura che ne consente l'autonoma sostituzione periodica da parte del singolo operatore - di norma il codice identificativo personale fornito ad ogni operatore non viene assegnato a persone diverse; - i supporti rimovibili e le copie di sicurezza	Poco probabile	Gravi	**BASSO**

				vengono custoditi in luogo non accessibile a persona diversa dall'incaricato del trattamento - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative *Trattamento senza strumenti elettronici* - gli incaricati al trattamento sono autorizzati al trattamento dei soli dati la cui conoscenza sia strettamente necessaria per lo svolgimento dell'incarico affidato o per l'espletamento delle competenze attribuite alla struttura organizzativa di riferimento - divieto di richiedere, raccogliere e/o conservare in fascicolo dati personali non pertinenti con le competenze e le attività svolte o eccedenti le necessità istruttorie delle attività assegnate - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative - il trasporto di dati personali all'esterno dei locali ove si svolge il trattamento, ma comunque all'interno dell'Azienda avviene in modo da garantirne la riservatezza			
Trattamento non conforme alla finalità della raccolta o illecito	Poco probabile	Gravi	Rilevante	*Trattamento con strumenti elettronici* - è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, dati non più occorrenti vengono di norma cancellati o distrutti (anche facendone richiesta all'Amministratore di Sistema, ove	Poco probabile	Gravi	**BASSO**

				il soggetto responsabile non fosse in possesso delle necessarie abilitazioni); qualora fossero conservati, non sono comunque utilizzabili. *Trattamento senza strumenti elettronici* - i dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo - è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, i documenti riportanti dati non più occorrenti - se non protocollati e/o allegati in fascicolo - vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili - i supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di un eventuale riutilizzo; se ciò non è possibile devono essere distrutti			

2) Misure di sicurezza tecniche e organizzative in via di implementazione o di prossima attuazione

Descrizione del rischio	**Opzioni che permettono di ulteriormente evitare o mitigare il rischio**
Danneggiamento/ perdita/distruzione non autorizzata dati personali	sistematizzare l'emanazione di indicazioni atte a responsabilizzare gli utenti interni sui rischi connessi all'utilizzo degli strumenti elettronici (ad esempio, rischi derivanti dalla tenuta ed archiviazione di dati sui rispettivi hard disk) e sui comportamenti, accorgimenti e misure da adottare per limitare/abolire danni correlati
Accesso non autorizzato dati personali	- sistema di tracciabilità degli eventuali accessi di personale non-CED - utilizzo di codici identificativi personali che non consentano l'accesso contemporaneo alla stessa applicazione da diverse stazioni di lavoro

	- definizione di istruzioni per l'uso, la custodia e la distruzione dei supporti rimovibili o del contenuto degli stessi, al fine di evitare accessi non autorizzati e trattamenti impropri - apposizione di clausole di sicurezza ai contratti di manutenzione software – ove non già esistenti - impostazione del controllo degli accessi sugli apparati di rete - totale sostituzione degli apparati privi di management
Trattamento non autorizzato (comprensivo di modifica, divulgazione……)	disattivazione dei codici personali nel caso in cui vi sia perdita della qualità che permette l'accesso all'operatore o di mancato utilizzo superiore ai sei mesi
Trattamento non conforme alla finalità della raccolta o illecito	- adozione di tecniche di cifratura o codici identificativi o di altre soluzioni che rendano temporaneamente inintelligibili i dati anche a chi è autorizzato ad accedervi, e permettano di identificare gli interessati solo in caso di necessità - trasferimento cifrato dei dati sensibili e giudiziari in formato elettronico (già attivo per VPN) - conservazione separata dei dati idonei a rivelare lo stato di salute e la vita sessuale rispetto ad altri dati personali oggetto di trattamento

3) Misure ulteriori a tutela della privacy e della riservatezza nell'esercizio della professione sanitaria e delle attività correlate

- chiamata degli interessati prescindendo dall'individuazione nominativa degli stessi in caso di prenotazione e attesa
- accorgimenti utili al rispetto delle distanze di cortesia
- soluzioni atte a garantire la riservatezza dei colloqui
- cautele volte ad evitare che la prestazione, ivi compresa l'anamnesi, avvengano in condizioni di promiscuità
- garanzie di informativa ai soli terzi legittimati in ordine alle prestazioni eseguite, previo consenso degli interessati
- procedure atte a prevenire esplicite correlazioni fra l'interessato e reparti/strutture indicative di un particolare stato di salute
- tutela della dignità della persona,
- divieto di affissione di liste di ospiti/utenti in locali aperti al pubblico
- evitare la visibilità ad estranei di documenti sulle condizioni cliniche dell'interessato
- rilasciare informazioni sullo stato di salute a persone diverse dall'interessato solo dietro acquisizione di specifico consenso (anche rilasciato da persone legittimate a farlo in caso di impossibilità o incapacità dell'interessato) e solo per il tramite di un medico designato dall'interessato, o dal responsabile del trattamento dei dati (individuato – per i dati di carattere sanitario e per le cartelle cliniche - nel Direttore Medico e nel Direttore del Laboratorio di Analisi, per quanto di rispettiva competenza): quest'ultimo può autorizzare a ciò per iscritto operatori sanitari diversi dai medici che, nell'esercizio dei propri compiti, intrattengano rapporti diretti con i pazienti, individuando nell'atto di incarico appropriate modalità e cautele
- divieto per i soggetti esterni di effettuare fotografie e/o riprese video di persone ed ambienti senza preventivo formale assenso rispettivamente da parte degli interessati e dei responsabili di struttura

Aggiornamento al 29.05.2020
Sostituisce la precedente versione del 11.03.2019, conservata in atti aziendali

Allegato

Azienda di Servizi alla Persona
"GOLGI - REDAELLI"

Regolamento UE 2016/679 – D. Lgs. 196/2003 smi –
Protezione delle persone fisiche con riguardo al trattamento dei dati personali

Valutazione d'impatto sulla protezione dei dati – DPIA

Attività di trattamento: Prestazioni legate a servizi riabilitativi dell'età evolutiva
Soggetti interessati: Soggetti minori affetti da disturbi del comportamento e dello spettro autistico; parenti, familiari, care givers, amministratori di sostegno, curatori, tutori.

Gentile Signora, Egregio Signore
L'ASP Golgi-Redaelli, Titolare del Trattamento, sta conducendo ai sensi delle vigenti norme una valutazione relativamente agli eventuali rischi per i diritti e le libertà delle persone fisiche ed ai possibili impatti derivanti dal trattamento dei dati per il quale Lei ha prestato il relativo consenso, e a tal fine ritiene di consultare le opinioni delle parti interessate.
Le Sue opinioni, raccolte in forma anonima con il presente breve questionario, contribuiranno a fornire elementi utili alla formulazione della valutazione in questione.
La preghiamo di restituire il presente documento alla segreteria del Servizio una volta compilato.
Si ringrazia per la collaborazione che riterrà di fornire.

Il Direttore Generale

QUESTIONARIO

Richiamate le informazioni rese disponibili dall'Azienda precedentemente all'inizio del trattamento (Informativa - Registro delle attività di trattamento), **ritiene che le attività di trattamento dei dati per l'effettuazione delle prestazioni legate a servizi riabilitativi dell'età evolutiva** poste in essere dall'ASP Golgi-Redaelli:

- siano effettivamente necessarie e che il trattamento sia proporzionato in relazione alle finalità perseguite

  SI ☐ NO ☐

- siano lecite e rispettose dei principi di correttezza e trasparenza

  SI ☐ NO ☐

- prevedano misure di protezione dei dati idonee ad attenuare i rischi per i diritti e le libertà delle persone fisiche interessate al trattamento (sicurezza fisica e dei dati di identificazione o attinenti l'identità personale; materiali (perdite finanziarie o al patrimonio); morali o biologici (turbamento per la diffusione di una notizia riservata, compromissione di uno stato di salute, evento lesivo di diritti umani o integrità della persona); sociali (conseguenze di tipo discriminatorio, perdite di autonomia)).

  SI ☐ NO ☐

data_____