Procedura "Protezione dati personali e tutela della riservatezza riferibili al Residente e al personale dipendente – Gestione Data Breach"

Sommario

1 - SCOPO e CAMPO DI APPLICAZIONE 2
2 - RESPONSABILITA' 2
3 - RIFERIMENTI NORMATIVI 5
4- ABBREVIAZIONI, TERMINI E DEFINIZIONI 5
5- MODALITA' OPERATIVE 6
TRATTAMENTO DATI DIPENDENTI 6
TRATTAMENTO DATI RESIDENTI 9
5 – MAPPA SISTEMA INFORMATIVO 12
6 - ALLEGATI E DOCUMENTI DI REGISTRAZIONE 13
1. Informativa al trattamento dei dati ai dipendenti (allegato nr. 1) 13
2. Informativa utenti (allegato nr. 2) Consenso al trattamento dati (Allegato nr.2).. 13
3. Disciplinare aziendale (alleg. nr. 3) 13
4. Istruzione Data breach (allegato nr. 4)..... 13

REV.	DATA	ELABORATA DA	VERIFICATA DA	APPROVATA DA
04	22/7/22	Ass. Amministrativo Daniela Debertolis Consulente Serv. DPO Avv. Grazioli	Upipa Serv. Dpo	Direttore Dott. ssa Federica Taufer
		Responsabile Qualità: Daniela Debertolis		Firma:

DISTRIBUZIONE

La presente procedura viene distribuita in copia alle seguenti figure professionali:

- **Coordinatore/Infermiere/i/Fisioterapista/O.S.S./Animatrice/ Personale Amministrativo**
- **Originale presso ufficio responsabile Qualità. Una copia rimane a disposizione del personale presso :**
  - sala del personale/riunioni

LISTA DELLE REVISIONI

REVISIONE N.	DATA	DESCRIZIONE DELLE MODIFICHE
00	28.05.2013	Prima emissione approvata dalla Direzione
01	09.05.2014	Aggiornamento contenuti
02	30.04.2019	Adeguamento al GDPR e al d.lgs 101/18
03	12/12/2019	Inserimento alleg. proc. data breach – revisione allegati (ambito e incarico unico doc.)
04	22/07/2022	Modifica punto 4) dell' istruzione del data breach Allegato nr. 4 "notifica della violazione al Garante"

1 - SCOPO e CAMPO DI APPLICAZIONE

La presente procedura definisce le responsabilità in merito al trattamento dei dati personali trattati dall'ente nell'esercizio dei propri compiti istituzionali affinché questo si svolga nel rispetto della normativa vigente nonché dei diritti e delle libertà fondamentali, della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

La presente procedura è stata elaborata tenuto conto del concetto di "acccountability" derivante dal Regolamento UE 16/679.

Scopo della presente procedura è quello di garantire che il trattamento dei dati personali acquisiti dell'ente sia disciplinato in modo tale da assicurare un elevato livello di tutela dei diritti e delle libertà di cui sopra nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per favorire l'adempimento degli obblighi di legge da parte del titolare del trattamento, A.P.S.P. "San Giuseppe" di Primiero e dei suoi preposti.

La presente procedura è applicata per la gestione del trattamento dei dati riferibili a:

- ✓ Utenti
- ✓ Dipendenti

2 - RESPONSABILITA'

La responsabilità legata alla presente procedura è affidata al Direttore dell'Ente e al Coordinatore Sanitario designati in ragione delle rispettive competenze quali soggetti delegati a talune operazioni di trattamento secondo le indicazioni del primo comma dell'art. 2 - quaterdecies del Codice in materia di protezione dei dati personali (si rimanda alla documentazione agli atti per l'evidenza di quali siano le rispettive funzioni e competenze).

Nell'ottica di implementare un modello organizzativo che tiene conto del concetto di "responsabilizzazione", al Direttore dell'Ente sono state assegnate le seguenti competenze:

- operare attivamente affinché nel contesto delle attività di trattamento svolte nell'area amministrativa dell'Ente siano rispettate da parte del personale coinvolto le regole e le disposizioni previste dal Regolamento UE 16/679 e dal Codice in materia di protezione dei dati personali;

- fornire supporto al titolare affinché sia data applicazione al principio di "minimizzazione" favorendo la riduzione dell'utilizzo di dati personali e identificativi in modo da escludere il loro trattamento quando le finalità perseguite possono essere realizzate mediante dati anonimi o modalità che consentano di identificare l'interessato solo se necessario;

- individuare le persone autorizzate a trattare i dati personali degli interessati con i quali l'ente si rapporta verificando che ognuna di esse abbia ricevuto appropriate istruzioni su come proteggere i dati e un'idonea autorizzazione a poter compiere specifiche attività di trattamento. In caso negativo, provvedere affinché ciò venga portato a compimento. Si ricorda che tutte le persone coinvolte in operazioni di trattamento dovranno attenersi con

scrupolo alle seguenti prescrizioni: sono consentite unicamente operazioni di accesso ai dati per finalità connesse all'adempimento delle prestazioni di competenza del singolo incaricato così come indicato nel documento di autorizzazione elaborato dal titolare. Eventuali diverse operazioni di trattamento sono tassativamente vietate. Nel dettaglio sono assolutamente vietate la comunicazione a terzi non legittimati o la diffusione, tramite qualsiasi mezzo, di dati personali di qualsiasi natura provenienti dai data base del titolare;

- verificare periodicamente che il processo di trattamento, diffusione ed archiviazione dei dati personali svolto nell'ambito di competenza sia coerente con il fine della loro protezione in modo tale da ridurre al minimo il rischio che i dati trattati possano andare persi, distrutti o entrare in possesso di terzi non autorizzati;

- verificare che il trattamento dei dati acquisiti sia sempre rispettoso delle finalità della raccolta;

- verificare che agli interessati sia stata somministrata l'informativa prevista dall'art. 13 del Regolamento UE e, laddove necessario, sia stato acquisito il loro consenso al trattamento;

- provvedere all'individuazione dei soggetti delegati a compiere determinate operazioni, segnalandone gli estremi al titolare in modo tale che nei loro confronti si possa procedere con la designazione quali responsabili del trattamento;

- coordinarsi con il responsabile della protezione dei dati segnalando a tale figura ogni ipotesi di criticità, vulnerabilità e violazione per consentire gli adempimenti di conseguenza;

- coadiuvare il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 (Sicurezza del trattamento), 33 (Notifica di una violazione dei dati personali all'autorità di controllo), 34 (Comunicazione di una violazione dei dati personali all'interessato), 35 (Valutazione d'impatto sulla protezione dei dati) e 36 (Consultazione preventiva), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

- verificare la conformità del trattamento svolto mediante videosorveglianza.

Al Coordinatore Sanitario sono state affidate le seguenti attività:

- operare attivamente affinché nel contesto delle attività di trattamento svolte nell'area socio sanitaria e assistenziale dell'Ente siano rispettate da parte del personale coinvolto le regole e le disposizioni previste dal Regolamento UE 16/679 e dal Codice in materia di protezione dei dati personali;

- sia data applicazione al principio di "minimizzazione" favorendo in ambito socio assistenziale e sanitario la riduzione dell'utilizzo di dati personali e identificativi in modo da escludere il loro trattamento quando le finalità perseguite possono essere realizzate mediante dati anonimi o modalità che consentano di identificare l'interessato solo se necessario;

- individuare le persone autorizzate a trattare i dati personali degli interessati con i quali l'ente si rapporta verificando che ognuna di esse abbia ricevuto appropriate istruzioni su come proteggere i dati e un'idonea autorizzazione a poter compiere specifiche attività di

trattamento. In caso negativo, provvedere affinché ciò venga portato a compimento. Si ricorda che tutte le persone coinvolte in operazioni di trattamento in ambito socio sanitario e assistenziale dovranno attenersi con scrupolo alle seguenti prescrizioni: sono consentite unicamente operazioni di accesso ai dati per finalità connesse all'adempimento delle prestazioni di competenza del singolo incaricato così come indicato nel documento di autorizzazione elaborato dal titolare. Eventuali diverse operazioni di trattamento sono tassativamente vietate. Nel dettaglio sono assolutamente vietate la comunicazione a terzi non legittimati o la diffusione, tramite qualsiasi mezzo, di dati personali di qualsiasi natura provenienti dai data base del titolare;

- verificare periodicamente che il processo di trattamento, diffusione ed archiviazione dei dati personali svolto nell'ambito socio assistenziale e sanitario sia coerente con il fine della loro protezione in modo tale da ridurre al minimo il rischio che i dati trattati possano andare persi, distrutti o entrare in possesso di terzi non autorizzati;

- verificare che il trattamento dei dati acquisiti, con particolare attenzione quando questi possano afferire informazioni sullo stato di salute, sia sempre rispettoso delle finalità della raccolta;

- verificare che agli interessati sia stata somministrata l'informativa prevista dall'art. 13 del Regolamento UE e, laddove necessario, sia stato acquisito il loro consenso al trattamento;

- provvedere all'individuazione dei soggetti delegati a compiere determinate operazioni, segnalandone gli estremi al titolare in modo tale che nei loro confronti si possa procedere con la designazione quali responsabili del trattamento;

- coordinarsi con il responsabile della protezione dei dati segnalando a tale figura ogni ipotesi di criticità, vulnerabilità e violazione per consentire gli adempimenti di conseguenza;

- operare affinché siano rispettate le indicazioni prescritte nelle Linee guida in materia di Dossier sanitario del 4 giugno 2015 del Garante per la protezione dei dati personali verificando che i trattamenti realizzati presso l'Ente mediante lo strumento del "dossier sanitario" o del "fascicolo sanitario elettronico" siano conformi alle predette indicazioni supportando attivamente il Titolare in ogni eventuale implementazione;

- adottare nel contesto dell'erogazione dei servizi assistenziali e sanitari le misure volte ad eliminare o, comunque, a ridurre al minimo qualsiasi rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio anche attraverso idonee procedure di valutazione di impatto;

- predisporre e verificare periodicamente lo stato di applicazione nel contesto dell'erogazione dei servizi assistenziali e sanitari del titolare di un idoneo sistema di sicurezza relativamente ai trattamenti svolti da parte di tutte le persone autorizzate tale da rispettare le prescrizioni di legge e le indicazione dell'Autorità garante;

- coadiuvare il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 (Sicurezza del trattamento), 33 (Notifica di una violazione dei dati personali all'autorità di

controllo), 34 (Comunicazione di una violazione dei dati personali all'interessato), 35 (Valutazione d'impatto sulla protezione dei dati) e 36 (Consultazione preventiva), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

3 - RIFERIMENTI NORMATIVI

- 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;
- 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)" (in G.U. 4 settembre 2018 n.205);
- Provvedimento del Garante privacy "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018). provvedimento Garante Privacy in materia di amministratore di sistema;
- provvedimento Garante in materia di videosorveglianza;
- provvedimento Garante in materia di fascicolo sanitario elettronico/dossier sanitario elettronico.

4- ABBREVIAZIONI, TERMINI E DEFINIZIONI

Ai fini della presente procedura si intende per:
a) **"trattamento",** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
b) **"dato personale",** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
c)"**categoria particolare di dati personali",** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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;
d) "**titolare del trattamento",** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici

applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
e) **"responsabile del trattamento",** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
f) "**destinatario",** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
g) **"incaricati",** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
h) **"interessato",** la persona fisica cui si riferiscono i dati personali;
i) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acqui- site di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
l) **«dati biometrici»: i** dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
m) **«dati relativi alla salute»:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
n) **"comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
o) **"diffusione",** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
p) "**autorità di controllo**", l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

5- MODALITA' OPERATIVE

TRATTAMENTO DATI DIPENDENTI

- Il Collaboratore Amministrativo referente del personale, su incarico del Direttore consegna l'incarico al trattamento ove è definito l'ambito del trattamento con le relative istruzioni operative sviluppato per categorie omogenee per mezzo della quale si autorizzano del trattamento i dipendenti e collaboratori dell'ente nonché gli altri soggetti che, in ragione dell'attività svolta, potrebbero avere la necessità di trattare dati personali, secondo le categorie uniformi (secondo comma art. 2- quaterdecies Codice privacy, comma 4 art. 32 RegUe 16/6769). L'incarico dovrà essere firmato per accettazione dal dipendente/addetto.

- Ai dati personali possono avere accesso solo soggetti incaricati in ragione di specifiche necessità derivanti dalla funzione svolta. L'elenco dei soggetti coinvolti viene ad essere descritto nel Registro dei trattamenti (agli atti). Ciascun incaricato è autorizzato a compiere le operazioni di trattamento necessarie ed indispensabili per adempiere ai compiti cui affidatario entro i limiti definiti nel proprio profilo autorizzativo.
- Il responsabile del sistema informatico provvede a definire i profili di autorizzazione e quindi l'accesso ai dati personali in base al ruolo ricoperto da ciascun soggetto autorizzato.
- Nell'adempimento dell'incarico conferito tutti i soggetti coinvolti sono tenuti ad attenersi ai principi di necessità indispensabilità. Ciascun incaricato è stato istruito sul fatto di dover trattare i dati ai quali ha accesso esclusivamente per lo svolgimento dei compiti e delle funzioni cui affidatario senza poter porre in essere alcuna nuova o diversa operazione di trattamento senza la preventiva autorizzazione del titolare nel pieno rispetto delle prescrizioni del Regolamento UE 16/679.
- Ogni attività deve essere svolta riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, con particolare attenzione quando questi possano rientrare nella "categoria particolare di dati personali", in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
- Agli incaricati si consegna il materiale formativo e le istruzioni operative allegate all'ambito; viene inoltre condiviso un disciplinare aziendale alleg. nr. 3 riferito al corretto utilizzo degli strumenti informatici.
- Periodicamente si organizzano sessioni formative in materia di protezione dati personali coinvolgendo se del caso il DPO e l'amministratore di sistema.
- Il rispetto da parte dei soggetti autorizzati delle indicazioni operative e delle istruzioni loro conferite viene ad essere verificato costantemente da parte del Direttore e del Coordinatore.
- Il collaboratore amministrativo distribuisce l'informativa al trattamento dei dati ai dipendenti (allegato nr. 1), ai liberi professionisti dell'ente e ai tirocinanti con attestazione della ricevuta di avvenuta consegna.
- Il trattamento dei dati personali relativi al personale dell'ente, gestiti dal Collaboratore Amministrativo addetto all'Ufficio gestione del personale, viene eseguito sia in modalità elettronica mediante utilizzo di strumenti informatici che in modalità cartacea (raccolta, registrazione, conservazione, utilizzo dei documenti mediante fascicoli, schede raccoglitori e archivi) e consiste nella trascrizione su cartaceo e nella conservazione nei locali dell'ente. In esecuzione ad obblighi di legge o di regolamento i dati personali dell'interessato potranno essere diffusi tramite sul sito internet dell'ente secondo la normativa vigente in materia; non è prevista diffusione dei dati riferiti allo stato di salute. I dati comunicati non saranno trasferiti verso Paesi Terzi o organizzazioni internazionali extra UE.
- Il trattamento a cui sono e saranno sottoposti i dati personali acquisiti nell'ambito della gestione del rapporto di lavoro (dati anagrafici, dati di contatto, dati identificativi, ecc.) ha le seguenti finalità: instaurazione e gestione del rapporto con il personale dipendente; adempimento di obblighi fiscali e contabili; applicazione della legislazione previdenziale e assistenziale; trattamento giuridico ed economico del personale; adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali; igiene e sicurezza del lavoro.

- I dati acquisiti vengono trattati nel rispetto delle misure di sicurezza tecniche e organizzative previste dal Regolamento UE attraverso procedure adeguate a garantire a riservatezza degli stessi. Tali misure sono oggetto di una costante attività di verifica e implementazione anche mediante il coinvolgimento dell'amministratore di sistema e la supervisione del DPO.
- Il trattamento dei predetti dati è indispensabile per consentire il perseguimento di finalità istituzionali proprie della APSP e dare adempimento agli obblighi previsti dalla normativa vigente.
- Il titolare del trattamento è impegnato nell'applicazione dei principi di indispensabilità e necessità nel trattamento. La raccolta e le operazioni di trattamento si limitano a quelle strettamente indispensabili per il perseguimento dei fini di cui legittimato. I dati personali sono:
  - ✓ trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
  - ✓ raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
  - ✓ adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
  - ✓ esatti e, se necessario, aggiornati;
  - ✓ conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
  - ✓ trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Nel trattamento, nella archiviazione e nella distruzione vengono rispettati i seguenti criteri:
- i dati personali dei dipendenti sono archiviati in cartelle chiuse e non trasparenti, contenute in armadi presso l'ufficio personale;
- i documenti contenenti dati personali sono utilizzati in modo tale da evitare che possano essere visionati da personale esterno;
- eventuali stampati contenenti dati personali vengono strappati prima di essere smaltiti;
- l'accesso ai computer è protetto da password personale e riservata soggetta a periodico aggiornamento;
- i locali in cui sono presenti dati personali sono in ogni caso presidiati da personale dell'Ente durante l'eventuale presenza di soggetti esterni.

Nei confronti di tale attività di trattamento l'ente ritiene di dover eseguire una valutazione di impatto tenuto conto dell'art. 35 del Reg. Ue 16/679 e delle indicazioni fornite dall'autorità Garante nel provvedimento "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018). Tale valutazione di impatto è attualmente oggetto di definizione con il coinvolgimento del DPO e verrà costantemente monitorata.

I dati acquisiti non saranno trasferiti in Paesi extra UE e saranno conservati nel rispetto dei termini di legge.

- In caso di ipotesi di violazione della sicurezza, l'ente provvede alla gestione del "data breach", come indicato negli artt. 33 e 34 del Reg. Ue 16/679 mediante una idonea

procedura elaborata con la condivisione e la supervisione del DPO (procedura agli atti allegato nr. 4).

- Relativamente ai dati conferiti, l'interessato o un suo rappresentante può esercitare, senza particolari formalità, i diritti previsti dagli artt. 15 e segg. del Regolamento UE 16/679 rivolgendosi al titolare o al responsabile per la protezione dei dati.
- La base giuridica del trattamento tiene conto di quanto indicato dall'art. 2-ter del codice in materia di protezione dati personali (Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).

TRATTAMENTO DATI RESIDENTI

- L'impiegato amministrativo che si occupa della gestione degli utenti è tenuto a consegnare l'informativa (allegato nr. 2) al momento della raccolta delle informazioni di pre ingresso.
- Al momento del colloquio di pre ingresso l'impiegato amministrativo dovrà acquisire il consenso al trattamento dati (parte finale informativa Allegato nr. 2) nel quale quali verranno indicati i nominativi dei soggetti ai quali l'ente è autorizzato a fornire informazioni. In caso di impedimento da parte del residente il modulo di consenso va firmato da parte di una figura esercitante legalmente la potestà, famigliare, prossimo congiunto, convivente o responsabile della struttura. Originale dello stesso rimarrà nel fascicolo dell'ospite presso l'ambulatorio infermieristico in apposito armadio e una copia presso il fascicolo amministrativo in deposito presso l'ufficio ospiti.
- I dati acquisiti vengono trattati nel rispetto delle misure di sicurezza tecniche e organizzative previste dal Regolamento UE attraverso procedure adeguate a garantire a riservatezza degli stessi. Tali misure sono oggetto di una costante attività di verifica e implementazione anche mediante il coinvolgimento dell'amministratore di sistema e la supervisione del DPO.
- Il trattamento dei predetti dati è indispensabile per consentire il perseguimento di funzioni istituzionali proprie della APSP e, nello specifico, per le seguenti finalità: permettere l'instaurazione, gestione e amministrazione del rapporto; dare esecuzione di obblighi contrattuali e di legge; consentire la programmazione e pianificazione delle attività; favorire la gestione del contenzioso; organizzare servizi di controllo interni (della sicurezza, della qualità dei servizi, dell'integrità del patrimonio, degli ingressi e delle uscite anche mediante predisposizione e attivazione di pertinenti sistemi di contenzione personale); svolgere analisi statistiche o attività di ricerca (mediante dati anonimi); permettere l'erogazione di servizi infermieristici, fisioterapici, medici e sanitari e prestazioni di prevenzione, diagnosi, cura, riabilitazione a tutela dell'incolumità fisica e della salute dell'interessato e di terzi; favorire la comunicazione delle informazioni dello stato di salute dell'interessato a soggetti terzi legittimati; permettere l'erogazione dei servizi a favore degli interessati in condivisione o in contitolarità con altri soggetti (medici, farmacisti, liberi professionisti, operatori servizi sociali, enti territoriali, ecc.) per esigenze di cura e amministrative strettamente correlate alla attività sopra indicata; garantire la fornitura di servizi assistenziali, infermieristici o sanitari su delega o in convenzione con la APSS.
- Il titolare del trattamento è impegnato nell'applicazione dei principi di indispensabilità e necessità nel trattamento. La raccolta e le operazioni di trattamento si limitano a quelle strettamente indispensabili per il perseguimento dei fini di cui legittimato. I dati personali sono:
  - trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

❖ I dati non saranno trattati mediante processi decisionali automatizzati. Tutti i dati conferiti sono trattati secondo i principi di correttezza, liceità e trasparenza sia in forma cartacea che elettronica e protetti mediante misure tecniche e organizzative per assicurare idonei livelli di sicurezza ai sensi degli artt. 25 e 32 del GDPR.

❖ Il trattamento dei dati personali relativi ai residenti dell'ente in ambito sanitario viene eseguito sia in modalità elettronica mediante utilizzo di strumenti informatici che in modalità cartacea (raccolta, registrazione, conservazione, utilizzo dei documenti mediante fascicoli, schede raccoglitori e archivi) e consiste nella trascrizione su cartaceo e nella conservazione nei locali dell'ente. Non si effettua alcuna diffusione dei dati stessi. Nel trattamento, nella archiviazione e nella distruzione vengono rispettati i seguenti criteri:

- i dati personali dei residenti sono archiviati in cartelle chiuse e non trasparenti, contenute in armadi presso l'ambulatorio infermieristico e utilizzati in modo tale da evitare che possano essere visionati da personale esterno;
- eventuali stampati contenenti dati personali vengono strappati prima di essere smaltiti;
- l'accesso ai computer è protetto da password personale e riservata soggetta a periodico aggiornamento;
- le informazioni relative ai residenti sono registrate e archiviate nel software denominato Cba, il quale consente l'accesso tramite password nonché l'autorizzazione degli accessi e delle visualizzazioni/inserimenti consentiti tramite diversi profili a seconda della figura professionale;
- il trattamento di dati personali, comuni e riferiti allo stato di salute, potrà essere effettuato, previo specifico consenso, attraverso procedure volte a informatizzare la gestione della cartella sanitaria. Tale modalità prevede l'elaborazione in formato elettronico delle informazioni inerenti lo stato di salute dell'interessato relativamente ad eventi clinici presenti e trascorsi (p.es.: referti, documentazione relativa a ricoveri, dati clinici, immagini di indagini diagnostiche, ecc.) al fine di permettere e documentare la storia clinica e migliorare le prestazioni di prevenzione, diagnosi e cura. Tale sistema prevede che dati comuni e riferiti allo stato di salute siano elaborati con modalità informatiche e allocati su banche dati idonee a rendere accessibile la consultazione, differenziata per ambiti specifici e profili di autorizzazione, da parte di personale incaricato al loro trattamento del rispetto dei principi di necessità, indispensabilità e pertinenza.
- Nello specifico, alle banche dati potrà avere accesso personale incaricato da parte dell'A.P.S.P. nonché, alla luce dell'attivazione del sistema TreC, da parte di eventuali soggetti incaricati al trattamento da parte della Azienda Provinciale per i Servizi Sanitari della Provincia Autonoma di Trento in riferimento alle distinte competenze e nel rispetto dei principi di pertinenza e necessità per le seguenti finalità: gestione

delle schede U.V.M., gestione anagrafica ospiti e predisposizione di piano assistenziale sintetico (software ATLANTE); refertazione esami di laboratorio e radiologici (sistema SIO); anagrafe provinciale esami laboratorio (sistema IPPOCRATE), prenotazione servizi CUP, gestione servizi decentrati (centro prelievi, fisioterapia, ecc.). Gestione sistema TreC (cartella clinica del cittadino). Il dossier o il fascicolo potrà essere consultato, anche senza il consenso dell'interessato, ma nel rispetto dell'autorizzazione generale del Garante, qualora sia indispensabile per la salvaguardia della salute di un terzo o della collettività.

- i locali in cui sono presenti dati sensibili dei residenti sono in ogni caso presidiati da personale dell'Ente durante l'eventuale presenza di soggetti esterni.
- Anche nei confronti di tale attività di trattamento l'ente ritiene di dover eseguire una valutazione di impatto tenuto conto dell'art. 35 del Reg. Ue 16/679 e delle indicazioni fornite dall'autorità Garante nel provvedimento "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018). Tale valutazione di impatto è attualmente oggetto di definizione con il coinvolgimento del DPO e verrà costantemente monitorata.
- I dati acquisiti non saranno trasferiti in Paesi extra UE e saranno conservati nel rispetto dei termini di legge.
- In caso di ipotesi di violazione della sicurezza, l'ente provvede alla gestione del "data breach", come indicato negli artt. 33 e 34 del Reg. Ue 16/679 mediante una idonea procedura elaborata con la condivisione e la supervisione del DPO (procedura agli atti).
- Relativamente ai dati conferiti, l'interessato o un suo rappresentante può esercitare, senza particolari formalità, i diritti previsti dagli artt. 15 e segg. del Regolamento UE 16/679 rivolgendosi al titolare o al responsabile per la protezione dei dati.
- La base giuridica del trattamento tiene conto di quanto indicato dall'art. 2-ter del codice in materia di protezione dati personali (Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).

5 – MAPPA SISTEMA INFORMATIVO

FASI	*ELEMENTI DEL SISTEMA INFORMATIVO*			
RACCOLTA E TRASFORMAZIONE DEI DATI IN INFORMAZIONI	**DATI**	**INFORMAZIONI**	**PERSONE**	**STRUMENTI**
INGRESSO UTENTE	dati anagrafici dell'utente dati bancari dell'utente raccolta consenso trattamento dati	creazione fascicolo utente	personale ufficio amministrativo	sistema informatico - SofwtwareC.S.S. programma CBA
	dati assistenziali dell'utente	creazione cartella sanitaria assistenziale dell'utente	personale addetto all'assistenza sociosanitaria dell'utente	sistema informatico - SofwtwareC.S.S. programma CBA
	dati sanitari dell'utente	raccolta ordine temporale dei referti di tipo diagnostico e terapeutico dell'utente divisi per tipologia		faldone cartaceo
ASSUNZIONE DI PERSONALE	dati anagrafici del neo assunto curriculum vitae dati bancari del neo assunto raccolta consenso informato e incarico trattamento dei dati	creazione fascicolo dipendente	personale ufficio amministrativo responsabile formazione	fascicolo cartaceo inserimento in anagrafica del personale programma informatico CBA e sito ECM Trento
ATTIVITA' AMMINISTRATIVA	raccolta dati dei fornitori	creazione elenco dei fornitori	personale ufficio amministrativo	sistema informatico
	raccolta dati beni acquistati	inventario beni	personale ufficio amministrativo	sistema informatico - Software Sipcar plus Programma C.B.A.
ATTIVITA' DI MONITORAGGIO DELLA SODDISFAZIONE ESTERNA	raccolta dati soddisfazione utenti	creazione fascicolo soddisfazione utenza	responsabile di servizio	sistema informatico
GESTIONE DATI E INFORMAZIONI:	**DATI**	**INFORMAZIONI**	**PERSONE**	**STRUMENTI**
ATTIVITA' EROGATA AGLI UTENTI	consultaizone quotidiana della cartella clinico assistenziale dell'utente registrazione quotidiana in cartella clinico assistenziale dell'utente	acquisizione delle nuove informazioni creazione di valutazioni multiprofessionali dell'utente	personale addetto all'assistenza sociosanitaria dell'utente	Software Sipcar plus Software Atlante
	consultazione referti inerenti il residente	acquisizione di nuove informazionei sanitarie diagnostico - terapeutiche	personale medico	Programma S.I.O.
ATTIVITA' CONTABILE	fatture emesse e ricevute, ordini a fornitori, dati bancari	bilancio d'esercizio, relazioni di gestione	personale ufficio amministrativo	sistema informatico - Software CBA Sipcar plus
	timbrature del personale	database mensile	personale ufficio amministrativo	sistema informatico - Programma C.B.A.
ATTIVITA' DI COMUNICAZIONE	comunicazioni in entrata / uscita (cartacee , elettroniche)	registrazione di lettere ed e-mail in entrata e uscita nel protocollo	personale ufficio amministrativo	programma CBA, archivio cartaceo delle comunicazioni
PRODUZIONE, EROGAZIONE, DIFFUSIONE, MESSA A DISPOSIZIONE DI INFORMAZIONI	**DATI**	**INFORMAZIONI**	**PERSONE**	**STRUMENTI**
INFORMAZIONI ALL'UTENZA	informazioni rispetto allo stato di salute e alla quotidiantià dell'utente	colloquio con utenti - famigliari - ammministratori di sostegno - tutori	medico, coordinatore, responsabili di servizio, infermieri, operatori	registrazione comunicazioni in CBA CSS
ATTIVITA' DI PUBBLICITA'	informazioni inerenti l'attività offerta e la regolamentazione della stessa	carta servizi, regolamenti, statuto, brochure, avvisi	personale dell'azienda ed esterni - potenziali utenti / fruitori dei servizi	pubblicazioini cartacee - pubblicazione sito internet aziendale
ATTIVITA' DI MONITORAGGIO	dati relativi l'andamento delle attività	report di monitoraggio dell'attività e relazioni	direzione - C.d.A. - referenti dei servizi	file di gestione dati in excel; estrapolazione dati dal SofwareCBA Programma C.S.S.; stampa di report cartacei
ATTIVITA' ORGANIZZATIVA	informazioni al personale delle modalità operative da adottare nelle varie fasi dell'attività	protocolli, procedure, istruzioni operative	tutto il personale coivolto da ogni documento	faldone cartaceo
	compiti ed orari del personale	piano delle attività	tutto il personale del settore socio - sanitario e assistenziale	documento cartaceo
ARCHIVIAZIONE DATI	**DATI**	**INFORMAZIONI**	**PERSONE**	**STRUMENTI**
USCITA DELL'UTENTE	dati anagrafici, sanitari, assistenziali e sociali dell'utente	fascicolo dell'utente e cartella sanitaria	personale ufficio amministrativo personale addetto all'assistenza sociosanitaria	faldoni cartacei; cartelle informatizzate CSS
RELAZIONI ATTIVITA' SVOLTA	dati inerenti l'attività	report, relazioni,	direzione	faldoni cartacei; cartelle informatizzate.
USCITA DEL PERSONALE	dati anagrafici, sanitari, assistenziali e sociali del dipendente	fascicolo del dipendente	personale d'ufficio	faldoni cartacei; cartelle informatizzate.

6 - ALLEGATI E DOCUMENTI DI REGISTRAZIONE

1. Informativa al trattamento dei dati ai dipendenti (allegato nr. 1)
2. Informativa utenti (allegato nr. 2) Consenso al trattamento dati (Allegato nr.2)
3. Disciplinare aziendale (alleg. nr. 3)
4. Istruzione Data breach (allegato nr. 4)