REGOLAMENTO INTERNO PRIVACY

Adottato dalla Casa di Cura Sanatorio Triestino, ai sensi del D.Lgs 30 giugno 2003, n.196 ("Codice in materia di protezione dei dati personali"), del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 e del D. Lgs. n.101/2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679)

Redazione:	Presidente CdA
Verifica:	dott.S.Guarneri, Ing.A.Catalani, DPO E.Morandini
Approvazione:	Presidente CdA
Pareri specialistici:	dott.P.Crismani, dott.a A.Sabot, dott.a S.Di Caccamo, sig. A.Zarri,

Modifiche rispetto alla versione precedente:

Aggiornamento Normativa

Il presente Regolamento sulla Privacy disciplina all'interno della struttura la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali, emanato con D.Lgs. del 30/06/2003 n.196 e in conformità all'emanazione della nuova normativa sovranazionale, il **Regolamento UE 2016/679 (GENERAL DATA PROTECTION REGULATION)** - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla loro libera circolazione - e della recente entrata in vigore del D. Lgs n.101/2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679).

Dall'esame della novità normativa emerge la necessità di un cambiamento di mentalità che porti alla piena tutela della privacy intesa non solo come un obbligo di rispetto di adempimenti burocratici ma, soprattutto, come garanzia per il cittadino che accede ai servizi delle strutture sanitarie di una riservatezza totale.
Uno strumento essenziale di sensibilizzazione è l'attività formativa del personale della struttura e l'attività informativa diretta a tutti coloro che hanno rapporti con la nostra realtà.

DEFINIZIONE ED OBIETTIVI

La procedura si propone di disciplinare il trattamento dei dati personali e di codificare i percorsi di autorizzazione al trattamento oltreché di individuare i luoghi presso cui viene conservata la documentazione, le misure di sicurezza messe in atto e quelle programmate per il futuro al fine del loro miglioramento.
Il presente manuale viene completato dall'Organigramma della Privacy della Casa di Cura Sanatorio Triestino che identifica il Titolare del trattamento, i Referenti Interni, il Responsabile della Protezione dei dati personali (Data Protection Officer: DPO) e gli Incaricati al trattamento dei dati; inoltre, dalla modulistica (nomine, informative e consensi, elenco fornitori esterni – responsabili/incaricati esterni –, registro delle attività, etc..).

TRATTAMENTO DEI DATI PERSONALI

Si intende 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:

- Raccolta
- Registrazione
- Organizzazione
- Strutturazione
- Conservazione
- Uso

- Adattamento o modifica
- Estrazione
- Consultazione
- Comunicazione mediante trasmissione
- Diffusione o qualsiasi altra forma di messa a disposizione
- Il raffronto o l'interconnessione
- Limitazione
- Cancellazione
- Distruzione

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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

- ✓ **Categorie particolari 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 o 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, il cui trattamento è vietato salvo eccezioni paragrafo 2 art.9 Regolamento UE.

- ✓ **Dati personali relativi a condanne penali e reati:** deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati Membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

In riferimento al trattamento di dati genetici, biometrici e relativi alla salute, il D.Lgs n.101/2018 non apporta sostanziali modifiche rispetto al Regolamento UE; si prevede tuttavia l'intervento prossimo del Garante con definizione di misure di garanzia specifiche.

INFORMATIVA (art. 13)

L'interessato deve essere previamente informato circa:

- l'identità e i dati di contatto del titolare del trattamento e del DPO;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- i soggetti o la categoria di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione del trattamento;

- le conseguenze di un eventuale rifiuto di rispondere → pregiudica la prestazione il rifiuto al trattamento dei dati personali; non pregiudica la prestazione il rifiuto al consenso per il DSE;
- qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e, in caso affermativo attraverso quali strumenti;

Il Regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente", in particolare:

- il periodo di conservazione dei dati personali;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto della portabilità dei dati;
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di presentare un reclamo all'Autorità di controllo.

CONSENSO (art.6)

Il Regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica: tra i fondamenti di liceità del trattamento l'acquisizione da parte dell'interessato di un consenso al trattamento dei suoi dati personali per una o più specifiche finalità.
Per i dati sensibili (dati sanitari, genetici e biometrici), deve avvenire per il tramite di una dichiarazione inequivocabilmente esplicita.

Il consenso:

- deve essere informato e quindi va espresso solo dopo aver letto l'informativa;
- deve essere libero, specifico e potrà essere revocato in ogni momento;
- è valido ed efficace fino a revoca (diritto di revoca che l'interessato può esercitare in qualsiasi momento).

Solo in caso di ricovero è prevista l'acquisizione del consenso ad ogni degenza; per tutte le altre prestazioni verrà richiesto di manifestare il consenso in un'unica dichiarazione in sede di primo accesso, fino a revoca dello stesso o a compimento del sedicesimo anno di età in caso di minore.

L'onere della prova dell'avvenuto consenso è a carico del titolare del trattamento, che deve essere in grado di dimostrare che l'interessato ha prestato il consenso ad uno specifico trattamento.

Non è necessario ed il trattamento è legittimo se funzionale ad adempiere un obbligo legale al quale il titolare è soggetto o se il trattamento è necessario per la salvaguardia di interessi vitali dell'interessato o di altra persona fisica.

Nel caso in cui l'interessato non possa dare il consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere e di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Il tutore, amministratore di sostegno o altro soggetto che abbia la legale rappresentanza dell'utente compilerà il modulo del consenso al trattamento dei dati intestandolo all'utente stesso e completandolo con i propri dati anagrafici e la propria firma; a richiesta esibisce la documentazione emessa dall'Autorità Giudiziaria.

In caso di persona assistita capace di intendere e volere ma con impedimento materiale alla firma, è necessario che l'acquisizione del consenso avvenga in presenza di due testimoni che debbono essere identificati a mezzo di documento di identità valido.

Il consenso dei minori è valido a partire dai 16 anni: prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci. Nello specifico, il consenso al trattamento dei dati di un minore inferiore ai 16 anni d'età deve essere firmato almeno da un genitore esercente la potestà genitoriale. In deroga a quanto sopra, sulla base della normativa specifica, il minore d'età superiore ai 14 anni può prestare in autonomia il proprio consenso al solo trattamento dei dati personali (non per il DSE), esclusivamente per le prestazioni previste dalle disposizioni a tutela della procreazione consapevole, per l'interruzione volontaria della gravidanza, per la prevenzione delle malattie sessualmente trasmissibili, per l'accertamento di abusi/atti di violenza, per gli accertamenti relativi al virus HIV (salvo richiesta di anonimato).

I SOGGETTI

Sono stati individuati ai sensi della normativa vigente le seguenti figure e i relativi responsabili a cui sono state date le istruzioni sui loro compiti e di cui è presente l'incarico nell'organigramma relativo alla privacy:

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*, *le modalità del trattamento* di dati personali *e i mezzi* utilizzati per farlo. Il titolare del trattamento dei dati personali è

Sanatorio Triestino S.p.A., nella persona del Presidente del CdA, in qualità di Rappresentante Legale della struttura.
Il titolare del trattamento pianifica, predispone e mette in atto misure tecniche e organizzative adeguate (privacy by design e by default) per garantire che siano trattati, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

- Il Titolare deve accertarsi che i **principi** applicabili al trattamento dei dati personali **siano rispettati.** Ovvero: i dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Le finalità devono essere determinate, esplicite e legittime; i dati: adeguati, pertinenti, esatti ed aggiornati, oltre che limitati a quanto necessario rispetto alle finalità, e comunque da trattare in modo da garantirne un'adeguata sicurezza. CAPO II ART 5

- Il Titolare deve distinguere i casi in cui per eseguire un trattamento è richiesto il (previo) **consenso dell'interessato**, da quelli in cui non è necessario acquisirlo. La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Quando per un trattamento è necessario il consenso, il titolare deve essere in grado di dimostrare che il consenso è stato effettivamente prestato. E' lecito se il minore che ha prestato il consenso ha **compiuto 16 anni**. In caso di minori di 16 anni, deve essere acquisito il consenso di colui/coloro che ha/hanno la responsabilità genitoriale del minore e il titolare deve adoperarsi in ogni modo ragionevole, in considerazione delle tecnologie disponibili, per verificare la detta circostanza. CAPO II ART 6,7,8

- Il Titolare tratta "particolari categorie di dati personali " (ex dati sensibili) e i dati relativi a condanne penali e reati unicamente in determinate **condizioni** che, in relazione all'aspetto sanitario sono : consenso esplicito dell'interessato, interesse vitale dello stesso, finalità di medicina preventiva o del lavoro, per motivi di interesse pubblico nel settore della sanità pubblica, ai fini di ricerca scientifica. Inoltre è consentito per queste finalità solo laddove i dati siano trattati da o sotto la responsabilità di un soggetto tenuto a segreto professionale.
  CAPO II ART 9,10

- **Trasparenza** nella gestione dei trattamenti: il titolare è tenuto ad adottare misure appropriate per fornire all'interessato tutte le informazioni/comunicazioni relative ai trattamenti gestiti dalla propria organizzazione, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. E' tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato

ritardo e comunque entro un mese dal ricevimento della medesima (prorogabile di due mesi ove necessario, tenuto conto della complessità e del numero delle richieste). CAPO III ART 12

- **Informativa all'interessato:** adempimento basilare per qualsiasi titolare, l'informativa richiesta dal Regolamento UE è più ricca di informazioni della precedente, per esempio, il titolare deve esplicitarvi il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo. Non in ultimo, il linguaggio dell'informativa deve essere semplice e chiaro (dettagli in seguito) CAPO III ART 13,14

- **Il rispetto dei diritti dell'interessato**: il Regolamento UE formalizza un ampio catalogo di diritti che spettano all'interessato. Si tratta del diritto di accesso, del diritto di rettifica, del diritto alla cancellazione (più noto come diritto all'oblio), diritto di limitazione (oscuramento) del trattamento, diritto alla portabilità dei dati, diritto di opposizione al trattamento, con gli eventuali connessi obblighi di notifica/comunicazione gravanti sul titolare. Nel caso di processi decisionali automatizzati è riconosciuto il diritto dell'interessato a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato dei dati che produca effetti giuridici che lo riguardano o che comunque incida significativamente sulla sua persona (tra le operazioni contemplate dalla norma campeggia la *profilazione* come definita dall'art. 4.1, n. 4). Il correlativo divieto non si applica ove la decisione si basi sul consenso esplicito dell'interessato, sia necessaria per l'esecuzione di un contratto con l'interessato, ovvero sia autorizzata dal diritto dell'Unione o del singolo Stato membro. CAPO III ART 13,14,15,16,17,18,20,21

- **Misure di sicurezza adeguate**: il titolare del trattamento deve adottare misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità del trattamento al Regolamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure debbono essere periodicamente riesaminate e aggiornate. CAPO IV ART 24, 32

- **Privacy by design** (fin dalla progettazione): tenendo conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche, all'atto del trattamento ovvero di determinare i mezzi del medesimo il titolare adotta misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati. CAPO IV ART 25.1

- **Privacy by default** (per impostazione predefinita): attua misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi. CAPO IV ART 25.2

- **Contitolarità del trattamento**: nel caso in cui due o più titolari operino come contitolari del trattamento (determinando congiuntamente finalità e mezzi del medesimo), concordano in modo trasparente, mediante un contratto, la ripartizione delle responsabilità del trattamento, con particolare riguardo all'esercizio dei diritti degli interessati e ai connessi obblighi informativi. Il contenuto essenziale dell'accordo deve essere messo a disposizione degli interessati. CAPO IV ART 26

- **Nomina del Rappresentante del titolare**: laddove si applichi l'art. 3.2 (trattamento di dati personali relativi ad interessati che si trovano nell'Unione da parte di titolare/responsabile non stabilito nell'UE), il titolare/responsabile designa per iscritto un proprio rappresentante nell'Unione. Il rappresentante è l'indefettibile interlocutore della competente autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento. CAPO IV ART 27

- **Nomina del Responsabile del trattamento**: il titolare può nominare un Responsabile Interno (o più) che effettui il trattamento per suo conto. Il titolare ha la responsabilità di scegliere per tale incarico un soggetto/organismo che presenti garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate. Nonché di fornire a lui ed a tutti gli incaricati adeguata formazione ed istruzioni **(obbligo di istruzione)** CAPO IV ART 28, 29

- **Adozione del Registro delle attività di trattamento**: è adempimento obbligatorio per il titolare del trattamento con almeno 250 dipendenti o che, anche al di sotto di tale soglia dimensionale, effettui un trattamento che possa presentare un rischio per i diritti e le libertà degli interessati che non sia occasionale o che includa dati sensibili, genetici, biometrici, giudiziari. Cuore del documento è una mappa dettagliata di tutti i trattamenti effettuati dall'organizzazione del titolare. CAPO IV ART 30

- **Obbligo di cooperazione con l'autorità di controllo**: è tenuto a cooperare con l'autorità di controllo, quando quella gliene faccia richiesta. IV - 31

- **Notificazione di una violazione dei dati**: rientra tra gli obblighi del titolare anche la notifica all'autorità di controllo (Garante) senza ingiustificato ritardo - e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza - di ogni violazione della sicurezza dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche. IV - 33

- **Comunicazione di una violazione dei dati all'interessato**: quando la violazione della sicurezza dei dati presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve darne notizia all'interessato senza ingiustificato ritardo. La norma fissa i requisiti di contenuto della comunicazione, che deve essere redatta con un linguaggio semplice e chiaro. Altresì la norma individua i casi in cui la detta comunicazione non è richiesta (per semplicità, quando il titolare ha adottato misure tali da scongiurare il rischio o quando la comunicazione richiederebbe sforzi sproporzionati). IV - 34

- **Redazione della Valutazione d'impatto sulla protezione dati- DPIA (data protection impact assesment) e consultazione dell'autorità di controllo**: si tratta di un ulteriore adempimento che grava sul titolare che debba iniziare un trattamento molto rischioso per i diritti e le libertà delle persone fisiche. Ciò si può verificare, in particolare, quando sia implicato l'uso di nuove tecnologie, ovvero in considerazione di altre caratteristiche (natura, oggetto, contesto, finalità) del trattamento. Quando la valutazione di impatto indichi che il trattamento presenta un rischio elevato, prima di procedere al trattamento il titolare è tenuto a consultare l'autorità di controllo. IV - 35, 36

- **Nomina di un Responsabile della Protezione dei Dati (DPO)**: il DPO ha compiti di informazione, formazione, consulenza e sorveglianza dell'adempimento della disciplina 'privacy'. E' anche l'interlocutore dell'autorità di controllo.

  La nomina del DPO è adempimento obbligatorio quando il titolare del trattamento:

  a) è autorità/organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali);

  b) effettua trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

  c) effettua come attività principali trattamenti su larga scala di dati sensibili, genetici, biometrici, giudiziari. IV, 37-39

- **Adesione a codici di condotta/sistemi di certificazione**: si tratta di adempimenti volontari del titolare mediante i quali può implementare importanti misure di sicurezza dei trattamenti e dimostrare la conformità delle attività di trattamento ai requisiti stabiliti dal Regolamento. IV - 40-42

- **Cautele per il trasferimento dei dati in Paesi terzi**: il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale deve essere effettuato nel rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dal Regolamento. V - 44, 45, 46, 47, 48, 49

- **Obbligo di risarcimento del danno**: il titolare è tenuto a risarcire il danno materiale o immateriale cagionato da una violazione del Regolamento. Egli è esonerato da tale responsabilità soltanto se dimostra che l'evento dannoso non gli è in alcun modo imputabile. VIII – 82

REFERENTE INTERNO DEL TRATTAMENTO

Si attiene alle istruzioni impartitegli per iscritto dal Titolare, vigila e collabora col Titolare affinché le disposizioni impartite, la presente policy aziendale ed il GDPR vengano rispettati all'interno dell'azienda. Ovvero deve assicurarsi che ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:

- **liceità**, vale a dire conformemente alle disposizioni alle norme di legge (in particolare il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume) e del Codice Etico;
- **correttezza**, nei confronti dell'interessato e della sua situazione, i dati debbono essere per tanto esatti;
- **trasparenza**, è necessario rendere consapevole l'interessato sugli scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- **aggiornamento**, è necessario cancellare o rettificare i dati inesatti rispetto alle finalità per cui sono trattati;
- **integrità**, debbono essere adottate le misure di sicurezza idonee a scongiurare trattamenti non autorizzati o illeciti, ovvero la perdita, la distruzione, il danno accidentale o la trasmissione a terzi non autorizzati;
- **responsabilizzazione**, ovvero è necessario progettare un modello organizzativo tale da conformare la gestione dei dati personali e sensibili alle finalità ed allo spirito del Regolamento UE 2016/679 e della normativa italiana vigente;
- **necessità**, i sistemi informatici ed i processi organizzativi debbono essere predisposti secondo la logica di riduzione al minimo dell'utilizzo delle informazioni personali ed identificative dell'individuo, in modo da escluderne il trattamento quando le perseguite nei singoli casi possono essere realizzate tramite dati anonimi;
- **finalità**, i dati possono essere trattati esclusivamente nell'ambito delle finalità che si intendono perseguire e delle quali gli interessati debbono essere puntualmente resi edotti (nello specifico: cura, ricerca, amministrativo-contabile e governo inteso come l'attività svolta dalle autorità di verifica sulla spesa sanitaria e sulla qualità delle prestazioni sanitarie);
- **minimizzaizone**, possono essere raccolti e trattati solo i dati necessari per lo scopo specifico perseguito dal titolare ed impiegati solo per il periodo strettamente necessario per il raggiungimento del suddetto scopo, al termine del quale non debbono essere più resi disponibili e conservati non oltre i termini di legge.

Ciascun trattamento nell'area di competenza deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare:

→ identificare e censire, monitorare e riferire sui trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;

→ eseguire una valutazione dei rischi e suggerire al Titolare eventuali adeguamenti (tecnici ed organizzativi) al fine di ridurre eventuali rischi residui;

→ verificare, per ciascun trattamento di dati personali, la minimizzazione del trattamento e di conservazione del dato, garantendo la cancellazione o l'anonimizzazione dei dati obsoleti;

→ ogni qualvolta si raccolgano, nell'Area a Lei afferente, dati personali accertarsi a che venga fornita un'adeguata informativa ai soggetti interessati, suggerirne la modifica qualora fosse necessario;

→ far osservare gli adempimenti previsti dal Titolare in caso di richiesta di oscuramento, modifica e cancellazione di trattamenti applicando le corrette procedure previste per tali attività;

→ far rispettare tutte le misure minime di sicurezza richieste espressamente dal Codice Privacy (art 83) ed allegato B di tipo "fisico" e "tecnico", già disposte da Titolare (es. uso di un adeguato sistema di credenziali di autenticazione- da non divulgare in modo alcuno-, blocco dello schermo e degli applicativi qualora ci si allontani dalla postazione di lavoro, corretta archiviazione in luoghi inaccessibili della documentazione cartacea);

→ collaborare col Titolare nel definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati eseguendo verifiche periodiche nell'area di competenza, ai fini di testare la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico (max 7 gg);

→ verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative disposte dal Titolare, la loro applicazione ed eventualmente suggerirne di nuove e più efficaci;

→ assicurare che nelle sale d'attesa la chiamata degli interessati deve prescindere dalla loro individuazione nominativa (salvo esplicita autorizzazione scritta);

→ verificare il rispetto delle predisposte appropriate distanze di cortesia;

→ evitare che le prestazioni sanitarie avvengano in situazioni di promiscuità;

→ prevenire una diretta correlazione tra l'interessato e ambulatorio/reparto indicativo di un particolare stato di salute;

→ vigilare che i soggetti autorizzati afferenti alla Sua area anche qualora non siano tenuti per legge al segreto professionale applichino regole di condotta analoghe al segreto professionale così come disposto dal titolare;

→ verificare e poi relazionare il Titolare mediante un aggiornamento almeno annuale dell'ambito di trattamento consentito agli incaricati afferenti alla Sua Area *(la lista degli incaricati, redatta per classi omogenee di incarico e relativi profili di autorizzazione, verrà conseguentemente aggiornata dal Titolare, sulla base delle Sue indicazioni);*

→garantire la custodia ed il controllo diligente di atti e documenti contenenti dati sanitari (in modo che non vi abbiano accesso persone prive del corretto profilo autorizzativo → accesso controllato agli archivi su autorizzazione preventivamente concessa);

→ Assiste il Titolare del trattamento nel predisporre un'**Informativa** secondo le norme individuate del **RGPD** (in particolare quelle relativi al Capo III – Diritti dell'interessato) e, all'occorrenza, promuoverne modifiche ed integrazioni qualora mutassero finalità, tecnologie utilizzate o altro.

Infatti l'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati per iscritto circa:

1. l'identità e i dati di contatto del Titolare e del DPO;

2. le finalità (diagnosi e cura, amministrativo-contabili, ricerca e governo) e le modalità (strumenti informatici/cartacei) del trattamento cui sono destinati i dati;

3.Il periodo di conservazione dei dati personali, oppure, se non è possibile, i criteri per determinare tale periodo;

4. la natura obbligatoria o facoltativa del conferimento dei dati;

5. le conseguenze di un eventuale rifiuto di rispondere;

6. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

7. i diritti di cui agli artt.13 ss RGDP: di chiedere al titolare del trattamento l'accesso ai dati personali, e la rettifica o la cancellazione degli stessi ("diritto all'oblio") o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

8. il diritto di proporre reclamo ad un'Autorità di controllo;

→ agevolare gli Interessati nell'esercizio dei loro diritti (di cui sopra) con particolare riguardo alla trasparenza e tracciabilità degli accessi;

→ nel momento in cui il Sanatorio Triestino adotterà il Dossier Sanitario Elettronico (DSE) Le verrà richiesta collaborazione per redigere un'attenta e preventiva DPIA (valutazione d'impatto) ed in una seconda fase, redigere adeguata informativa per il DSE;

→ comunicare immediatamente al Titolare ogni violazione (DATA BREACH) o mancata attivazione di quanto previsto dal GDPR e dal Regolamento privacy Aziendale relativamente al settore di competenza. Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.

INCARICATO INTERNO DEL TRATTAMENTO

Pur non prevedendone espressamente la figura, il Regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".
Sono incaricati di svolgere le operazioni di trattamento dei dati personali di loro competenza con l'indicazione dei compiti, dell'ambito di trattamento consentito e delle modalità (informative per gruppi omogenei di funzioni, in base alle attività che svolgono).

La designazione degli incaricati al trattamento dei dati personali è di competenza del Responsabile, tramite una nomina effettuata per iscritto che ne individua i compiti e le modalità cui deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito.

L'incaricato collabora con il Titolare ed il Responsabile segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.

In particolare, l'incaricato deve assicurare che, nel corso del trattamento, i dati siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
- raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile on tali modalità
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità pel quali i dati sono trattati;
- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita , dalla distruzione o dal danno accidentale.

L'Incaricato è tenuto alla completa riservatezza sui dati di cui sia venuto a conoscenza in occasione dell'espletamento della sua attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e dal Responsabile, nei soli casi previsti dalla legge e/o nello svolgimento dell'attività istituzionale dell'Azienda.

Gli Incaricati devono ricevere idonee ed analitiche istruzioni, anche per gruppi omogenei di funzioni, riguardo le attività sui dati affidate (inserimento, aggiornamento, cancellazione, ecc.) e gli adempimenti cui sono tenuti.

RESPONSABILI DEL TRATTAMENTO

Tutti i soggetti esterni che effettuano operazioni di trattamento sui dati della struttura, per conto e nell'interesse della stessa, per finalità connesse all'esercizio delle funzioni istituzionali.

E' la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento,designato direttamente da quest'ultimo tramite contratto che dimostra di presentare garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile esterno decide solo i mezzi del trattamento e risponde in via solidale con il titolare.

Il titolare del trattamento dei dati deve informare ciascun responsabile delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da atto scritto che vincola il responsabile del trattamento al titolare del trattamento e che stabilisce la durata, la natura e le finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del responsabile del trattamento.

I responsabili del trattamento rispondono al titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata adozione delle misure di sicurezza.

I responsabili esterni devono:

- trattare i dati personali solo su istruzione del titolare del trattamento;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare il tempestivo ed integrale rispetto dei doveri dell'azienda previsti dal Regolamento, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art.32 del Regolamento UE 2016/679;
- osservare le disposizioni della presente policy, nonché delle specifiche istruzioni impartite dal titolare;
- adottare misure idonee per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del garante e da quelle contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che incidono sul trattamento dei dati:

  - ✓ articolo 5 della legge 5 Giugno 1990, n. 135 per la tutela della riservatezza della persona affetta da infezione da HIV;
  - ✓ legge 22 Maggio 1978, n. 194 per le comunicazioni sulle interruzioni di gravidanza;
  - ✓ articoli 120 e 121 del DPR 9 Ottobre 1990, n. 309 in materia di tossicodipendenze;
  - ✓ articoli 5 e 5- bis del decreto legge 17 Febbraio 1998, n.23, convertito nella legge 8 Aprile 1998, n.94, in materia di sperimentazione clinica in campo oncologico;
  - ✓ articolo 734- bis c.p. concernente il divieto di divulgazione non consentita dell'immagine delle persone offese da atti di violenza sessuale.

- assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento UE 2016/679 (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione

d'impatto sulla protezione dei dati ed ev. consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nella presente Policy;
- contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

La designazione del/dei responsabili esterni viene effettuata mediante atto di nomina del titolare da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente alla struttura.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico tra le parti.

INCARICATO ESTERNO DEL TRATTAMENTO

Tutti coloro che svolgono un'attività di trattamento dei dati, pur non essendo dipendenti della struttura, devono essere incaricati tramite una lettera di nomina come incaricati esterni.

Sono soggetti agli stessi obblighi cui sono sottoposti tutti gli incaricati, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

Nel caso di incaricati esterni, l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

La designazione viene effettuata da parte del Responsabile (interno o esterno) mediante atto di nomina scritto.

DPO (Data Protection Officer)

Il Responsabile della Protezione dei dati deve essere designato obbligatoriamente dal titolare e dal responsabile – in funzione della sua conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali – ogni qual volta il trattamento riguardi categorie particolari di dati personali, al fine di facilitare l'osservanza delle disposizioni del RGPD.

Il Titolare del trattamento o il Responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

Il DPO deve disporre di autonomia e risorse sufficienti a svolgere efficacemente i suoi compiti e può avere il supporto di un team di collaboratori.

Il DPO non risponde di persona in caso di inosservanza del Regolamento UE ma l'onere di assicurare il rispetto della normativa in materia di protezione dei dati spetta al titolare.

IL REGISTRO DELLE ATTIVITA'

Il titolare del trattamento e ciascun responsabile del trattamento istituiscono un registro delle attività di trattamento svolte sotto la propria responsabilità, che deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo.

Il registro <u>del titolare</u> deve contenere almeno:

a) Il nome e i dati di contatto del Titolare del trattamento e, se nominati, del contitolare del trattamento, del rappresentante del titolare del trattamento e del DPO;
b) Le finalità del trattamento;
c) Una descrizione delle categorie di interessati e delle categorie dei dati personali;
d) Le categorie di destinatari a cui i dati personali sono o saranno comunicati, compresi i destinatari di Paesi Terzi od Organizzazioni Internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) dove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) dove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il registro <u>del responsabile</u>

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (ART.20)

La valutazione dell'impatto dei trattamenti sulla protezione dei dati personali va realizzata, prima di procedere al trattamento, dal titolare quando un tipo di trattamento, considerata la natura, il contesto, la finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il titolare del trattamento definisce a priori un elenco delle tipologie di trattamenti soggetti al requisito della valutazione d'impatto, nello svolgere la quale si consulta con il responsabile della protezione dei dati; il DPO può essere chiamato ad esprimere un parere.

La valutazione deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, incluse 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 e delle altre persone in questione.

Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il titolare, se necessario, procede ad un riesame della valutazione d'impatto sulla protezione dei dati.

IL FASCICOLO SANITARIO ELETTRONICO

Attualmente in fase di test presso la ns azienda sanitaria di afferenza, non ci vede ancora coinvolti, ma con prospettiva di imminente realizzazione.

Il Fascicolo Sanitario Elettronico (Fse) è una vera e propria infrastruttura digitale: è l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito e originati da diversi titolari del trattamento solitamente operanti in un medesimo ambito territoriale (es., aziende sanitarie, centri privati accreditati, laboratori ecc operanti nella medesima regione o area vasta).

Il nucleo minimo di dati e documenti inseriti nel FSE è costituita da:

- ✓ dati identificativi e amministrativi dell'assistito
- ✓ referti
- ✓ verbali di pronto soccorso
- ✓ lettere di dimissione
- ✓ profilo sanitario sintetico
- ✓ dossier farmaceutico
- ✓ consenso o diniego alla donazione di organi e tessuti

Le finalità che possono essere perseguite attraverso la costituzione del Fse possono essere ricondotte esclusivamente a finalità di cura dell'interessato e cioè di prevenzione, diagnosi, cura e riabilitazione, studio e ricerca, con esclusione di ogni altra finalità, ferme restando eventuali esigenze in ambito penale.

Qualora attraverso il FSE si intendano perseguire talune finalità amministrative connesse all'erogazione della prestazione sanitaria richiesta dall'interessato, i dati amministrativi devono essere separati dalle informazioni sanitarie, prevedendo profili diversi di abilitazione degli operatori in funzione della differente tipologia di attività ad essi consentite.

All'interessato deve essere garantita la facoltà di scegliere se far costituire o meno un Fse con le informazioni sanitarie che lo riguardano, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista che li ha redatti, senza la loro necessaria inclusione all'interno del Fse.

Il consenso deve essere autonomo e specifico e preceduto da un'idonea informativa, formulata in modo chiaro, che evidenziare che il mancato consenso alla costituzione del Fse, non incide sulla possibilità di usufruire delle prestazioni mediche richieste e di poter accedere comunque alle prestazioni del Servizio sanitario nazionale. L'informativa e la connessa manifestazione del consenso possono essere formulate distintamente per ciascuno dei titolari del trattamento, in modo cumulativo, avendo comunque cura di indicare con chiarezza l'ambito entro il quale i singoli soggetti trattano i dati inseriti nel Fse. Il consenso eventualmente prestato dall'interessato si distingue in generale (espresso al momento della costituzione del Fse) e specifico (prestato ai fini della consultazione o meno da parte dei singoli titolari del trattamento). In determinate circostanze, se può essere consultato anche senza il consenso dell'interessato ma su autorizzazione generale del Garante qualora sia indispensabile per la salvaguardia della salute di un terzo o della collettività.

La normativa vigente prevede il diritto dell'interessato di oscurare alcuni eventi clinici che lo riguardano. L'"oscuramento" dell'evento clinico (revocabile nel tempo) deve peraltro avvenire con modalità tali da garantire che, almeno in prima battuta, tutti (o alcuni) soggetti abilitati all'accesso non possano venire automaticamente (anche temporaneamente) a conoscenza del fatto che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento").
Resta ferma la possibilità per il titolare del trattamento di informare i soggetti abilitati ad accedere a tali strumenti che tutti i fascicoli cui hanno accesso possono non essere completi, in quanto l'interessato potrebbe aver esercitato il suddetto diritto di oscuramento.

Inoltre, sulla base di un consenso informato e specifico dell'interessato, è possibile effettuare l'inserimento, all'interno del Fse, delle informazioni sanitarie pregresse alla costituzione del Fse che lo riguardano ed anche di quei dati che, per la loro natura, prevedono un vero e proprio **diritto all'anonimato** (sieropositività, violenze sessuali, pedofilia, uso di stupefacenti e alcool, parto in anonimato)

L'accesso al trattamento di dati personali effettuato attraverso il Fse, deve essere consentito solo per fini di prevenzione, diagnosi e cura dell'interessato e unicamente da parte di soggetti operanti in ambito sanitario, con esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche e organismi amministrativi anche operanti in ambito sanitario. Analogamente, l'accesso è precluso anche al personale medico nell'esercizio di attività medico-legale (es. visite per l'accertamento dell'idoneità lavorativa o alla guida). Il Fse può essere consultato, salvo diversa volontà dell'interessato, da tutti quei professionisti che a vario titolo prenderanno in cura l'interessato, secondo modalità tecniche di autenticazione che consentano di autorizzare l'accesso al Fse da parte del medico curante.

Il Titolare deve valutare attentamente quali dati pertinenti, non eccedenti e indispensabili inserire nel Fse in relazione alle necessità di prevenzione, diagnosi, cura e riabilitazione, anche mediante un'organizzazione modulare di tali strumenti in modo da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni (e, quindi, al modulo di dati) indispensabili.

La particolare delicatezza dei dati personali trattati mediante il Fse impone l'adozione di specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza (art. 31 del Codice), ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 e ss.).

In caso di soggetti minorenni il consenso deve essere espresso da un genitore o tutore e, una volta raggiunta la maggiore età è necessario che l'interessato esprima nuovamente il consenso.

DOSSIER SANITARIO ELETTRONICO

Il DSE costituisce l'insieme dei dati personali sanitari, riguardanti l'interessato, generati da eventi clinici presenti e trascorsi, formati e trattati dalla struttura e messi in condivisione logica dai professionisti sanitari che hanno in cura il paziente, al fine di documentarne la storia clinica e di offrirgli un migliore processo di cura.

Includendo solo le informazioni cliniche derivanti dagli accessi del paziente nella nostra struttura, ne restiamo gli unici competenti quanto a gestione.

È costituito solo con il consenso dell'assistito o, in caso di minore o di persona sottoposta a tutela, con il consenso del rappresentante legale, previa consegna di una apposita informativa sulla formazione del DS e sul trattamento dei dati raccolti.

Nell'informativa, che deve essere facilmente consultabile dall'interessato anche dopo la prestazione del consenso, sono evidenziati i seguenti punti:

- la finalità del trattamento
- la modalità di espressione del consenso alla formazione del dossier
- la natura e la validità del consenso (valido fino a revoca espressa dell'interessato)
- i soggetti abilitati alla visualizzazione
- le conseguenze del mancato consenso al dossier o di modifica e/o revoca
- la possibilità che il dossier sia consultabile anche da parte dei professionisti in libera professione nella struttura
- la descrizione delle misure adottate dalla Casa di Cura per la protezione dei dati da specifici rischi di accesso non autorizzato e di trattamento non consentito insieme alle misure volte a garantire l'esattezza, l'integrità e la continuità della fruizione dei dati
- i diritti dell'interessato
- le modalità per la revoca del consenso in qualsiasi momento.

Il consenso dell'interessato alla costituzione del DSE viene manifestato alla struttura sottoscrivendo oltre al consenso generale anche quello specifico alla formazione dello stesso. Nel dossier potranno essere inserite le informazioni sanitarie relative ad eventi clinici pregressi alla costituzione dello stesso, previo consenso specifico ed informato dell'interessato. Le due tipologie di consenso per il pregresso e il futuro sono disgiunte ed autonome per cui l'interessato può decidere di prestare il consenso per entrambi o solo per il primo.

Il mancato consenso dell'interessato al trattamento dei dati personali, mediante DSE, non pregiudica l'accesso alle cure mediche richieste.
In determinate ipotesi il DSE può essere consultato anche senza il consenso dell'interessato in virtù di un'autorizzazione generale del Garante, qualora si renda necessaria la salvaguardia della salute di un terzo o della collettività.

L'interessato può decidere di oscurare alcuni dati o documenti sanitari consultabili tramite il DS; tale scelta non deve essere rilevabile (cd. oscuramento dell'oscuramento).

L'interessato ha diritto di conoscere gli accessi eseguiti sul proprio DS (tracciabilità) facendo richiesta al titolare del trattamento. I file di log devono registrare per ogni operazione di accesso al dossier effettuata da un incaricato, almeno le seguenti informazioni:

- il codice identificativo del soggetto incaricato che ha effettuato l'accesso;
- la data e l'ora di esecuzione
- il codice della postazione di lavoro utilizzata
- l'identificativo del paziente il cui dossier è interessato dall'operazione di accesso da parte dell'incaricato
- la tipologia di operazione compiuta sui dati (cancellazione, consultazione, etc..)

Si ritiene congruo che i log delle operazioni vengano conservati per un periodo non inferiore a 24 mesi dalla data di registrazione delle operazioni.

Il Sanatorio Triestino si ripropone di implementare un sistema di ***audit log*** attraverso degli *alert* (indicatori di anomalie) che individuino comportamenti anomali o rischi relativi alle operazioni eseguite dagli incaricati (ad es. relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi).

Il Titolare deve inoltre individuare criteri per la **separazione e cifratura** dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali.

Modalità di utilizzo della modulistica informativa per il trattamento dei dati personali

A tutti gli utenti che accedono per qualsiasi tipologia di intervento in Casa di Cura viene richiesta la firma del modulo di autorizzazione al trattamento dei dati sensibili che,

per gli ambulatoriali viene raccolto al momento dell'accettazione, per i ricoveri viene raccolto al momento del preoperatorio o, per i ricoveri internistici o medici, al momento dell'accettazione amministrativa.

Per i ricoveri, considerata la specificità del consenso che richiede autorizzazione ad informare i parenti sullo stato di salute, l'autorizzazione deve essere raccolta prima di ciascun accesso alla Casa di Cura.

I consensi al trattamento firmati sono conservati nella cartella clinica nel caso di pazienti ricoverati, sono invece conservati presso l'archivio della Casa di Cura per tutte le prestazioni ambulatoriali.

IL DATA BREACH

Per *violazione dei dati personali (data breach*) si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni. Un data breach, quindi, non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente). Il nuovo regolamento generale europeo prescrive specifici adempimenti nel caso di una violazione di dati personali.

- **Casi di notifica della violazione**

La normativa (GDPR) prevede **l'obbligo di comunicare alle autorità di controllo** (sul sito del Garante sono già presenti degli appositi moduli) la violazione dei dati solo se il titolare ritiene probabile che dalla violazione dei dati possano derivare **rischi per i diritti e le libertà degli interessati.** Tutti i titolari del trattamento sono soggetti alla norma. La notifica dovrà avvenire entro 72 ore e comunque "senza ingiustificato ritardo".

Se il titolare ritiene che il rischio per i diritti e le libertà degli interessati è elevato, allora si dovranno informare anche gli interessati, sempre "senza ingiustificato ritardo". Non è richiesta la comunicazione all'interessato nei casi indicati dall'art. 34, cioé quando:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Per valutare i fattori che determinano il rischio per le libertà e i diritti degli interessati, sono stati fissati i seguenti parametri:

- **tipo di "breach"**: il tipo di violazione è un parametro per la valutazione del rischio. La violazione dei dati sanitari di tutti i pazienti di un ospedale è ben diversa dalla perdita dei dati sanitari di un singolo paziente;

- **natura, numero e grado di sensibilità dei dati personali violati:** l'accesso al nome e all'indirizzo dei genitori di un figlio rappresenta un rischio diverso rispetto all'accesso da parte dei genitori naturali del nome e dell'indirizzo dei genitori adottivi;

- **facilità di associare i dati violati ad una persona fisica**: può accadere che i dati violati non siano facilmente riconducibili ad una determinata persona fisica;

- **gravità delle conseguenze per gli Interessati**: quando il titolare del trattamento percepisce il rischio che i dati oggetto della violazione possono essere utilizzati immediatamente contro gli Interessati (es. sostituzione di persona);

- **numero di Interessati esposti al rischio**: un parametro è sicuramente quello del numero degli Interessati potenzialmente coinvolti;

- **caratteristiche del titolare del trattamento**: un attacco ad una struttura ospedaliera certamente è diverso dall'attacco ad una piccola azienda.

A titolo esemplificativo, quindi, nel caso una media company perda il temporaneo accesso agli indirizzi email dei propri clienti a causa di un blackout, non sarà necessario procedere alla notifica dell'evento. Al contrario, la temporanea perdita di accesso ai dati sanitari dei pazienti di un ospedale, deve essere considerato un evento che pone a rischio (anche elevato) i diritti degli individui e dovrà perciò essere correttamente gestita ai sensi degli artt. 33 e 34 del GDPR.

Allo stesso modo, lo smarrimento di un CD o di una chiavetta USB contenente dati criptati indecifrabili da terzi, nel caso in cui la chiave crittografica sia nel possesso del titolare e questi possieda un backup di tali dati, potrebbe ritenersi non lesivo nei confronti degli interessati e quindi non obbligatoriamente notificabile. In caso invece la chiave crittografica non sia sicura o non esista un backup dei dati smarriti, sarà necessario attivare le procedure di notifica e comunicazione individuate.

- **Contenuto della notifica**

La notifica deve avere il contenuto previsto dall'art. 33 del GDPR:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

- descrivere le probabili conseguenze della violazione dei dati personali;

- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Link al modello per la notifica del data breach predisposto dal Garante Privacy: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5033588

- **Obbligo di documentazione**

In ogni caso i titolari dovranno opportunamente documentare le violazioni di dati personali subite, tramite un apposito registro delle violazioni, anche se non comunicate alle autorità di controllo, nonché le conseguenze e i provvedimenti adottati. Il titolare dovrebbe anche documentare nel registro le ragioni delle decisioni assunte, nei casi in cui non ha proceduto alla notifica, ha ritardato la notifica e nei casi in cui non ha comunicato la violazione agli interessati.

Tale documentazione dovrà essere fornita al Garante in caso di accertamenti.

- **Linee Guida**

Nelle linee guida, il Gruppo di lavoro Art. 29 sul data breach (Guidelines on Personal data breach notification under Regulation 2016/679, adottate il 3 ottobre 2017) ritiene che *debba considerarsi "a conoscenza" il titolare che abbia un ragionevole grado di certezza in merito alla verificazione di un incidente di sicurezza.* È evidente che, in base alle specifiche circostanze, mentre alcune violazioni saranno facilmente rilevabili, per altre sarà necessario instaurare un'indagine più approfondita. In questi casi, durante la fase di investigazione, il titolare può essere considerato come privo di un grado di conoscenza tale da far scattare immediatamente l'obbligo di notifica. Ciò precisato, il Gruppo sottolinea che il diligente comportamento del titolare sarà in ogni caso valutato sulla base della sua tempestiva attivazione in caso venga informato di una possibile infrazione. La fase investigativa, quindi, non deve essere abusata per prorogare illegittimamente il termine di notifica.

A tale considerazione si legano le raccomandazioni del Gruppo sia con riferimento alla struttura organizzativa predisposta dal titolare, sia in merito al ruolo del responsabile del trattamento in caso di data breach. In primo luogo, il Gruppo raccomanda ai titolari di

predisporre un piano di sicurezza che evidenzi le procedure organizzative interne da adottare nella gestione di eventuali violazioni e l'organigramma dei soggetti o dei livelli direttivi a cui è necessario fare riferimento per riportare l'accadimento.

In merito al responsabile, l'art. 33 dispone l'obbligo in capo a quest'ultimo di informare tempestivamente il titolare dell'avvenuta violazione. Interpretando questo assunto alla luce del rapporto che lega titolare e responsabile, il Gruppo evidenzia come, in linea di principio, il titolare debba considerarsi a conoscenza della violazione nel momento in cui il proprio responsabile ne sia venuto a conoscenza. Non deve quindi esistere alcuna dilazione temporale nelle comunicazioni tra titolare e responsabile, giacché questi viene considerato come estensione fisica dell'attività del titolare e fa perciò scattare automaticamente l'obbligo di notifica in capo al primo.

Su questo punto, le linee guida prospettano l'ipotesi che il responsabile, sulla base di specifica autorizzazione del titolare contrattualmente prevista, possa eseguire personalmente la notifica per conto di quest'ultimo. Ciò non toglie, è bene sottolinearlo, che le responsabilità nei confronti dell'autorità e degli interessati scaturenti dalla notifica o dalla sua mancanza, permangano in capo al titolare. In caso di negligenza, il responsabile potrà rispondere unicamente nei confronti del titolare.

IL SISTEMA DI VIDEOSORVEGLIANZA

Il trattamento dei dati personali effettuato tramite l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica; anche il nuovo Regolamento EU non si esprime con una specifica normativa. La normativa riguardante i sistemi di videosorveglianza è contenuta nel "Provvedimento in materia di videosorveglianza", emanato in data 8 aprile 2010 dal Garante della Privacy. Il nuovo Provvedimento Generale sostituisce quello emanato nel 2004, in virtù dell'aumento massiccio dell'utilizzo di tali sistemi da parte di soggetti pubblici e privati.

Attualmente il sistema di videosorveglianza in regime nella casa di Cura prevede che la registrazione delle telecamere avvenga con questa cadenza di orari:

- in area accettazione sono attive dalle h19 alle ore 7 dal lunedì al venerdì, h24 il sabato e la domenica;
- in Direzione sono attive dalle h20 alle h8 dal lunedì al sabato, h24 la domenica.

Tale organizzazione oraria, con lo scopo unico di prevenire/identificare reati o atti di vandalismo e quindi garantire la sicurezza, esclude di fatto la possibilità che pazienti e/o soggetti terzi possano essere oggetto della registrazione.

Gli impianti di videosorveglianza vengono segnalati tramite apposita cartellonistica a ridosso dell'area interessata ed in modo tale che risulti chiaramente visibile. La conservazione delle immagini avviene nel rispetto della normativa vigente.

E'in fase di predisposizione una policy dettagliata che sarà allegata a parte.

POLICY SULL'UTILIZZO DEI DISPOSITIVI ELETTRONICI E TECNICI AZIENDALI

Ex GDPR, Art 4 Job Act - L 300/70, Provvedimento 1/3/2007 Del Garante

Premesso che:

- Tutti i dipendenti e collaboratori del Sanatorio Triestino sono tenuti ad operare con diligenza per tutelare i beni aziendali, attraverso una condotta lecita e responsabile
- Gli strumenti dati in dotazione (apparecchiature elettromedicali, PC, internet, posta elettronica, fotocopiatrice, telefono ecc.) sono da ritenersi ad uso esclusivamente aziendale
- E' imperativo dunque evitare utilizzi impropri dei beni aziendali che possano essere causa di danno o di riduzione di efficienza, o comunque in contrasto con l'interesse della Società.
- In ottemperanza a quanto previsto dal GDPR tutti i log ai sistemi informativi aziendali vengono tracciati. L'Amministratore di Sistema infatti, per motivi di sicurezza informatica, esegue audit periodici - procedura dettagliata in seguito-
- L'accesso alla rete aziendale è protetto: devono essere utilizzati username e password
- L'accesso ai sistemi gestionali (Pepa e Sysdat) è protetto: è necessario l'uso di credenziali unipersonali con password segrete (di almeno 8 caratteri con 90 gg di durata max) che non debono in nessun caso essere comunicate o condivise
- È necessario eseguire il log out dal programma gestionale in uso prima di abbandonare la postazione di lavoro anche per breve tempo
- I PC procedono al blocco dello schermo dopo 5 minuti di inutilizzo con richiesta di reinserimento della pw di accesso
- Gli strumenti di lavoro (analogici e digitali) non debbono mai essere accessibili ai non autorizzati

Regole per l'utilizzo di Internet

L'uso di Internet nelle sue numerose funzionalità è consentito esclusivamente per gli scopi pertinenti con l'attività lavorativa. Nello specifico:

1. è ammessa solo la navigazione in siti (ad esempio quelli del Ministero della Sanità, degli Enti Previdenziali, Aziende Sanitarie, Mutue etc.) considerati come correlati con l'attività lavorativa
2. è vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Azienda come il download di file freeware e shareware (musicali, video, documenti da fonte incerta, file exe ecc), se non preventivamente autorizzato dal Referente Interno o dal DPO
3. è vietato trasmettere all'esterno documenti, procedure, file e, in generale, qualsiasi informazione di pertinenza aziendale anche se sul documento originale non è riportata la dicitura "riservato";
4. è altresì vietato ogni genere di upload sulla rete o su dispositivi personali di materiale aziendale;
5. è vietato lo scambio di qualsiasi materiale tramite servizi di condivisione di dati/rete (chat ecc);
6. è vietato l'accesso ai social (Facebook, Twitter, Instagram ecc) dalle postazioni aziendali;
7. è vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione;
8. è vietata la partecipazione a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) mediante pc aziendali;
9. è tassativamente vietato l'utilizzo delle risorse dei servizi aziendali per la memorizzazione di materiale privato, personale o non attinente all'attività lavorativa. Relativamente all'utilizzo dei singoli computer, si precisa che l'assegnazione della risorsa non ne comporta la privatezza, in quanto trattasi di strumento di esclusiva proprietà aziendale, e quindi i file memorizzati non sono né tutelati né garantiti dal Sanatorio Triestino.

Regole per l'utilizzo della Posta Elettronica

1. la posta elettronica deve essere utilizzata esclusivamente per motivi di servizio;
2. la personalizzazione dell'indirizzo non comporta la sua privatezza, in quanto trattasi di strumenti di esclusiva proprietà aziendale messi a disposizione del dipendente o collaboratore al solo fine dello svolgimento delle proprie mansioni lavorative.
3. E' fatto divieto di utilizzare le caselle di posta elettronica aziendale del dominio @sanatoriotriestino.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione della Direzione
4. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa del titolare della casella di posta, la stessa potrà essere consultata ed utilizzata dal Referente / Coordinatore per verificare il contenuto di messaggi rilevanti per lo svolgimento dell'attività lavorativa.

5. Ogni messaggio di posta deve recare, in calce, il nominativo, il ruolo/qualifica, i recapiti dell'operatore che lo invia. I messaggi inviati tramite posta elettronica aziendale (di servizio e/o nominative) devono riportare in calce il seguente testo o testo analogo:
   "Questa comunicazione deve considerarsi esclusivamente di carattere aziendale e non viene inviata a titolo personale. Il contenuto è riservato, indirizzato esclusivamente al destinatario e può contenere informazioni tutelate dal segreto professionale e strettamente confidenziali. Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento aziendale adottate in materia. Se lo avete ricevuto per errore, siete pregati di avvisare il mittente e cancellare l'originale ai sensi del D.Lgs. 1967/2003 e del GDPR. Ogni altro uso di questo messaggio è proibito".
6. Nel corpo della mail possono essere inseriti dei dati personali (limitandoli più possibile) ma tassativamente NON "particolari categorie di dati" ovvero: i dati sanitari delle persone assistite vanno trasmesse esclusivamente mediante allegato criptato. La chiave di cifratura va indicata al destinatario autorizzato (previa verifica dell'autorizzazione – ovvero della nomina) tramite altro mezzo di comunicazione (telefonicamente, via sms, fax ecc).
7. Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione come ad esempio appelli di solidarietà;
8. Non è ammesso l'utilizzo di sistemi di webmail personali e private su pc aziendali

BYOD – Bring Your Own Device

Si ricorda che le politiche aziendali del Sanatorio Triestino non permettono di utilizzare propri dispositivi personali in servizio. In nessun caso è consentita la trasmissione, l'acquisizione e la diffusione di dati personali o sanitari delle persone assistite per tramite di dispositivi personali (es. fotografie, whatsapp o sms con liste appuntamenti, referti, ecc.) a prescindere dal profilo autorizzativo del destinatario. L'uso promiscuo del cellulare aziendale dato in uso ai coordinatori è da considerarsi un benefit, fermo restando il divieto assoluto di divulgare o diffondere dati personali o sanitari delle persone assistite e di altri soggetti.

Regole per l'utilizzo di scanner, fotocopiatrici, telefoni aziendali

L'utilizzo di questi strumenti è autorizzato esclusivamente per scopi pertinenti l'attività lavorativa. E' vietato l'uso per scopi personali: in caso di scansioni queste potrebbero restare disponibili nel disposto all'uopo nella rete aziendale ed essere visibili agli autorizzati.

Il cellulare aziendale dato in uso ai Coordinatori anche per motivi privati ha valore di benefit.

Teleassistenza

L'attività di manutenzione (ordinaria e straordinaria) remota sui P.C. connessi alla rete aziendale ed i software gestionali in uso viene svolta da personale autorizzato e nominato dal Titolare (AdS e Responsabili/Incaricati esterni) che potrà utilizzare specifici software. Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware.

Rintracciabilità e conservazione dei file di log della navigazione internet

Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, memorizzano un giornale (file di log) contenente le informazioni relative ai siti che i P.C. aziendali hanno visitato. Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'utente, garantendo in tal modo il suo anonimato. I dati vengono conservati per 48 ore, l'eventuale prolungamento dei suddetti tempi di conservazione è eccezionale e può avere luogo solo in relazione ad esigenze tecniche o di sicurezza del tutto particolari (rilevazione di allert sicurezza).

L'accesso a questi dati è effettuato dall'AdS o da personale esterno incaricato alla gestione manutenzione del sistema informatico (vedasi elenco Responsabili e Incaricati esterni) a ciò espressamente autorizzato anche sotto il profilo privacy.

I sistemi software gestionali sono programmati e configurati in modo da conservare per 24 mesi i file di log, con credenziali di accesso, orari e attività effettuate (consultazione, modifica, cancellazione ecc).

Controlli

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, Sanatorio Triestino, una volta rilevato il potenziale pericolo effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

a. analisi aggregata del traffico di rete riferito all'intera struttura e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle finalità istituzionali);

b. emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti alla sede in cui è stata rilevata l'anomalia;

c. in caso di successivo permanere di una situazione non conforme, è possibile effettuare controlli circoscritti su singole postazioni di lavoro.

Il Sanatorio Triestino si riserva la possibilità di un intervento di controllo diretto qualora si verifichino situazioni di particolare "pericolosità" nell'utilizzo di strumenti elettronici che minacciano la sicurezza del sistema informativo. Tale situazione di estremo danno giustifica la mancata possibilità di procedere ad un avviso come evidenziato nei precedenti commi, dandone contestuale informazione all'utente stesso.

Provvedimenti disciplinari

Qualora le procedure indicate rilevino delle anomalie sull'utilizzo degli strumenti informatici che possano essere configurate quali attività non conformi, l'operatore coinvolto potrà essere oggetto di contestazione disciplinare. L'Azienda procederà altresì a segnalare, eventualmente, l'evento alle Autorità competenti, anche al fine di una potenziale valutazione del danno; qualora la tipologia, la quantità o la modalità di utilizzo improprio degli strumenti informatici siano tali da essere rilevanti ai fini del codice penale, provvederà obbligatoriamente ad effettuare specifica denuncia all'Autorità Giudiziaria.

BIBLIOGRAFIA

- Codice in materia di protezione dei dati personali, emanato con D.Lgs. del 30/06/2003 n.196;
- Regolamento UE 2016/679 (GENERAL DATA PROTECTION REGULATION);
- Provvedimento in materia di videosorveglianza 8 aprile 2010 pubblicato sulla Gazzetta Ufficiale n.99 del 29 aprile 2010.
- D.Lgs. n.101/2018 (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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

PROCEDURE OPERATIVE

→PROCEDURA IN CASO DI DATA BREACH

A chi è rivolta: a tutti gli attori coinvolti nell'organigramma privacy
A chi notificare il data breach (certo o presunto): al Referente Interno competente o al DPO che sono tenuti a darne immediato riscontro al Titolare.
Premettendo che non sempre il titolare, anche quando ha appurato con ragionevole certezza l'esistenza di una violazione, è già in possesso di tutti gli **elementi utili** per effettuare una descrizione completa ed esaustiva dell'infrazione, al fine di accelerare i tempi di accertamento questi sono i criteri di valutazione da adottare:

- ✓ **approssimazione**: il titolare che non sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione può comunicarne in prima battuta un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti
- ✓ **notificazione in fasi**: in questo caso il titolare, per la complessità o estensione della violazione, potrebbe non essere in grado di fornire con immediatezza all'autorità tutte le informazioni necessarie. Potrà allora ottemperare agli obblighi di notifica comunicando, dopo una prima e rapida notifica di alert, tutte le informazioni per fasi successive, aggiornando di volta in volta l'autorità sui nuovi riscontri
- ✓ **notifica differita:** il Regolamento prevede la possibilità di effettuare una notifica differita, dopo le 72 ore previste dall'art. 33. È il caso in cui, per esempio, un'impresa subisca violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al titolare e l'invio scaglionato di un numero elevato di notificazioni tra loro identiche, il titolare è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

Modalità di comunicazione all'interessato

Le linee guida, sulla base dell'art. 34, ricordano che devono sempre essere privilegiate modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti). Il messaggio dovrebbe essere comunicato in maniera evidente e trasparente.
Anche in questo caso, il Regolamento è attento a non gravare i titolari di oneri eccessivi prevedendo che, nel caso la segnalazione diretta richieda sforzi sproporzionati, questa possa essere effettuata attraverso una comunicazione pubblica. Si sottolinea però che anche questo tipo di comunicazione deve mantenere lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato. Così, mentre può ritenersi adeguata la comunicazione fornita attraverso evidenti banner o notifiche disposte sui siti web, non lo sarà se questa sia limitata all'inserimento della notizia in un blog o in una rassegna stampa.

→PROCEDURA DI ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Scopo della seguente procedura è di indicare la modalità operativa di esercizio dei diritti da parte dell'interessato.
Una volta richiesta la specifica modulistica presso la segreteria, l'Interessato può inoltrarla ai seguenti soggetti:

- DPO (Data Protection Officer) dpo@sanatoriotriestino.it
- al Referente Interno area Tecnica a.catalani@sanatoriotriestino.it
- al Referente Interno area Sanitaria/Amministrativa salvatore.guarneri@libero.it

Rintracciabili anche telefonicamente al numero 040/9409511
Azioni possibili: l'interessato, relativamente ai suoi dati presenti presso la struttura ha diritto di:

- accesso
- rettifica
- cancellazione, oscuramento, limitazione, opposizione
- portabilità

→PROCEDURA DI GESTIONE C.V. CANDIDATI

Lo scopo del documento è quello di fornire le modalità operative per la gestione delle attività di selezione del personale. I candidati hanno facoltà di invio dei curriculum vitae:

- ✓ tramite sito aziendale www.sanatoriotriestino.it
- ✓ di persona oppure via posta ordinaria (allegando informativa reperibile sul sito o in azienda) col consenso al trattamento debitamente firmato, presso la sede legale – via D. Rossetti 62 – 34141 Trieste

Le finalità di utilizzo dei dati ricevuti tramite cv è unicamente la selezione del personale.
A seconda dell'inquadramento professionale del candidato (amministrativo o sanitario) il cv sarà preso in carico dal Coordinatore di riferimento che procederà a visionarlo, a dargli una valutazione di massima su una scala da 1 a 10 in base all'esperienza professionale ed al percorso formativo del candidato. Si procederà poi ad archiviare il cv in forma digitale o cartacea inserendolo in un'apposita cartella digitale sul computer in uso al Coordinatore di Riferimento, nominandolo con data di ricezione, e punteggio, o una cartella fisica posta sotto chiave.
Nella necessità di reperire una figura professionale corrispondente ai cv ricevuti, verranno contattati i candidati con maggior punteggio per un colloquio di valutazione con il Coordinatore.
La conservazione del dato digitalizzato si protrae per 24 mesi (periodicamente vengono eliminati i cv più vecchi) quello cartaceo non appena digitalizzato (su hardware con accesso regolato da password unipersonale, firewall, antivirus in locale chiuso a chiave non accessibile al pubblico) viene distrutto con macchina tritura documenti.