REGOLAMENTO AZIENDALE IN MATERIA DI

PROTEZIONE DEI DATI

"AOPC- CATANZARO"

Adottato dall'AOPC-CATANZARO, ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali) e del GDPR (UE 2016/679) del Parlamento Europeo.

INDICE

INTRODUZIONE

Il presente Regolamento sulla privacy è uno strumento di applicazione del Decreto Legislativo 30 giugno 2003, n° 196 (il cosiddetto “Codice sulla privacy") e del Regolamento UE 2016/679, nell'ambito dell'organizzazione aziendale. Il presente aggiornamento del precedente Regolamento aziendale sulla Privacy del 28/10/2005, n. 1022 si è reso necessario per recepire in un unico testo l'intera normativa in tema di trattamento dei dati personali (D. Lgs. 196 del 30/06/2003), regolamenti e codici deontologici succeduti negli ultimi anni, direttive e linee guida del Garante, Direttive dell'UE 2000/58 (sulla riservatezza nelle comunicazioni elettroniche e il recente Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali), nonché alla libera circolazione di tali dati. Il Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante privacy. Dall'esame della materia emerge come sia, ormai, improcrastinabile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle strutture sanitarie, di una riservatezza totale dal punto di vista reale e sostanziale.

Il diritto alla privacy è un vero e proprio diritto inviolabile della persona, che non si limita alla tutela sola riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità. Si parla, infatti, di protezione della persona oltre che dei dati, nel pieno rispetto dell’Accountability; forte Responsabilizzazione a tutti i livelli organizzativi.

Per questi motivi, la cultura della privacy necessita di crescere e rafforzarsi, principalmente fra gli operatori della sanità, perché solo con la conoscenza dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di legge, nel trattamento di dati di competenza, con la consapevolezza di contribuire concretamente al miglioramento della qualità del rapporto con l'Utenza.

OGGETTO

Il presente Regolamento disciplina, all'interno dell'Azienda Ospedaliera di Catanzaro, la tutela delle persone e degli altri soggetti in ordine al trattamento dei dati personali, nel rispetto di quanto previsto, dal D. Lgs. 196/03 (finché non sarà sostituito) e dal GDPR.

Il presente regolamento aziendale viene redatto in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE 2016/679 del Parlamento Europeo, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

FINALITÀ

L'Azienda garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.

La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale. "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano"(art. 8, paragrafo 1, Carta dei diritti fondamentali dell'UE)

SENSIBILIZZAZIONE

L'Azienda sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza, integrità, disponibilità e resilienza, nonché a migliorare la qualità del servizio offerto all'Utenza.

A tal riguardo, uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale aziendale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Azienda. Per garantire la conoscenza capillare delle disposizioni del Codice e del presente Regolamento, al momento dell'ingresso in servizio è data a ogni dipendente una specifica comunicazione (con apposita clausola inserita nel contratto di lavoro) con i riferimenti per l'acquisizione del presente Regolamento, pubblicato sul sito aziendale, contenente tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale.

Il dipendente si impegna a scaricare copia, prenderne visione ed attenersi alle sue prescrizioni.

TITOLARE DEL TRATTAMENTO

II "Titolare" del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

"Trattamento": qualunque operazione effettuata con o senza l'ausilio di strumenti elettronici concernente la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, l'estrazione, l'utilizzo, la comunicazione, la diffusione, la cancellazione, la distruzione dei dati, anche se non registrati in una banca dati (Regolamento UE art.4).

Il Titolare del trattamento dei dati personali ai sensi e per gli effetti del Codice è l'AOPC-88100-Catanzaro, rappresentata dal Direttore Generale, in qualità di legale rappresentante dell'Azienda stessa, con sede in Via Vinicio Cortese n.25.

Il Titolare, avvalendosi della collaborazione del DPO, dopo averlo nominato, provvede:

- a richiedere al Garante per la protezione dei dati personali l'autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'obbligo di notificazione e comunicazione;
- a nominare con proprio atto i Responsabili del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della

Privacy , all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;

- a nominare l'Amministratore di Sistema;
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
- mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al presente Regolamento.

RESPONSABILI INTERNI DEL TRATTAMENTO DEI DATI PERSONALI

Ai fini del presente Regolamento s'intende per Responsabile:

"La persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione ed Organismo preposti dal Titolare al trattamento di dati personali.

Il Titolare (Direttore generale dell'AOPC), in considerazione della complessità e della molteplicità delle funzioni istituzionali dell'Azienda, designa quali Responsabili del trattamento interni le figure apicali che dirigono le strutture operative (complesse o semplici) al fine d i per mettere loro la messa in atto delle misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato (Regolamento UE 2016/679, art. 28):

Sono individuati quali Responsabili del trattamento:

- i Dirigenti Responsabili di Dipartimento, Presidio Ospedaliero, Struttura complessa/semplice e Struttura dipartimentale, per le banche dati cartolari e per le banche dati elettroniche delle singole strutture;
- il Dirigente Responsabile del Servizio informatico aziendale (SIA) per le banche dati elettroniche gestite centralmente;
- tutti i soggetti esterni che, in qualsiasi maniera, per svolgere la propria attività sulla base di convenzione/contratto con le Aziende che vengono in contatto con dati di cui è titolare l'Azienda, ma, soprattutto, se hanno un repository dei dati, a qualunque livello, dell'AOPC presso la loro Sede (Responsabili esterni).

Il Titolare del trattamento dei dati deve informare ciascun Responsabile del trattamento dei dati, così come individuato dal Regolamento, 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 del trattamento, la natura e la finalità del trattamento, il tipo dei dati personali e 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.

Il Responsabile del trattamento deve:

- 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 Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del Regolamento UE 2016/679;
- osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal Titolare;
- adottare idonee misure di Sicurezza 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, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati, e in particolare:
    - 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.
- Tenendo conto della natura del trattamento, assistere il titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
- 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, 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 nel presente Regolamento;
- 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.

Il Responsabile per il trattamento dei dati personali, nell'espletamento della sua funzione, collabora con il DPO al fine di:

- comunicare tempestivamente, l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell' osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE 2016/679 riguardanti: l'adozione di

misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato; la redazione della valutazione d'impatto sulla protezione dei dati; la consultazione preventiva;

- predisporre le informative previste e verificarne il rispetto e fornire le informazioni necessarie per l'aggiornamento del registro dei trattamenti;
- designare gli incaricati del trattamento, e fornire loro specifiche istruzioni;
- rispondere alle istanze degli interessati secondo quanto stabilito dal Codice e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
- segnala al DPO ogni modifica all'interno delle strutture organizzative dell'azienda o all'esterno (nuovi soggetti interni o esterni che trattano dati, nuovi trattamenti);
- garantisce che tutte le misure di sicurezza riguardanti i dati dell'Azienda siano applicate all'interno dell'Azienda stessa ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;
- informa il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

In allegato al presente Regolamento la lettera di nomina del Responsabile del trattamento fletterà di nomina del Responsabile interno (Allegato 1) e (Allegato 5) istruzioni per lo svolgimento delle operazioni di trattamento).

RESPONSABILI ESTERNI DEL TRATTAMENTO

Tutti i soggetti esterni che effettuano operazioni di trattamento sui dati dell'Azienda, per conto e nell'interesse della stessa, per finalità connesse all'esercizio delle funzioni istituzionali, sono nominati "Responsabili esterni" del trattamento, qualora siano in possesso dei requisiti previsti dall'art. 29, primo comma, del Codice (esperienza, capacità ed affidabilità).

I Responsabili esterni hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia di privacy;
- rispettare le misure di sicurezza previste dal Codice sulla privacy e adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
- nominare al loro interno i soggetti incaricati del trattamento;
- garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato del trattamento;
- trattare i dati personali, anche di natura sensibile e sanitaria, dei Pazienti esclusivamente per le finalità previste dal contratto o dalla convenzione;
- attenersi alle disposizioni impartite dal Titolare del trattamento;

- specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti; comunicare le misure di sicurezza adottate per garantire la riservatezza, l'integrità e la disponibilità nonché la protezione dei dati personali trattati.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata comunicazione, all'Ufficio Privacy, dell'atto di nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso l'Azienda, il Responsabile esterno del trattamento.

La designazione del Responsabile esterno viene effettuata mediante "atto di nomina" da parte del Titolare del trattamento da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente all'Azienda. L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

Nel termine di quindici giorni le strutture aziendali che hanno stipulato accordi o convenzioni con soggetti esterni all'Azienda devono far pervenire al DPO idonea informativa degli accordi stipulati che comportano il trattamento dei dati all'esterno dell'Azienda.

In caso di mancata comunicazione ne rispondono direttamente.

Entro 30 giorni dalla stipula del contratto, accordo o convenzione la struttura che ha stipulato l'accordo deve trasmettere alla Direzione Generale copia dell'atto di nomina del Responsabile del trattamento (interno/esterno) controfirmato per accettazione, informando il DPO dell'avvenuta ricezione.

INCARICATI INTERNI DEL TRATTAMENTO

"Gli incaricati" del trattamento sono le persone fisiche, dipendenti delle strutture sanitarie e amministrative, designati dal Responsabile del trattamento, incaricati di svolgere le operazioni di trattamento dei dati personali di sua competenza con l'indicazione dei compiti, dell'ambito di trattamento consentito, e delle modalità.

Ogni dipendente preposto ad un determinato servizio è tenuto ad effettuare operazioni tecniche di trattamento ed è da considerare, a tutti gli effetti, "Incaricato" ai sensi dell'art. 30 del Codice sulla privacy. La designazione dell'incaricato al trattamento dei dati personali è di competenza del Responsabile del trattamento; la nomina è effettuata per iscritto e individua puntualmente i compiti spettanti all'incaricato e le modalità cui deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

L'Incaricato collabora con il Titolare ed il Responsabile segnalando eventuali situazioni di rischio nel trattamento dei dati, 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 con tali finalità;
- 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 per 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 a cui sono tenuti.

INCARICATI ESTERNI DEL TRATTAMENTO

Tutti coloro che svolgono un'attività di trattamento dei dati, pur non essendo dipendenti dell'Azienda, che agiscano nel perimetro di sicurezza devono essere incaricati tramite una lettera di nomina come incaricati esterni (es. tirocinanti, volontari, borsisti che operano temporaneamente all'interno dell'Azienda o incaricati nominati dal Responsabile esterno).

Questi ultimi 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.

AMMINISTRATORE DI SISTEMA

L'Amministratore di Sistema, individuato dal dirigente della struttura complessa Sistemi informativi aziendali (SIA), sovrintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Azienda.

L'amministratore di sistema svolge attività, quali: il salvataggio dei dati, l'organizzazione del Disaster Recovery, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione, la

manutenzione hardware e la protezione logica dei Server e delle postazioni di lavoro (Firewall, antivirus, ID Penetration test) e propone al Titolare del trattamento un documento di valutazione del rischio informatico.

Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, gli Amministratori di Sistema devono adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (accesso log) devono essere complete, inalterabili, verificabili e la loro integrità deve soddisfare adeguatamente il raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.

La nomina dell'Amministratore di Sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza informatica e di reti. La designazione dell'Amministratore di Sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Secondo la normativa vigente, l'operato degli Amministratori di Sistema deve essere verificato, con cadenza annuale, da parte del Titolare del trattamento o dal Responsabile del trattamento a cui afferisce, in modo da controllare la sua rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.

L'Azienda applica quanto previsto dal Provvedimento del Garante della Privacy in materia di "misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, così modificato in base al provvedimento del 25 giugno 2009.

DATA PROTECTION OFFICER (DPO) - Responsabile dei Protezione Dati

(Regolamento UE 2016/679 artt. 37,38 e 39)

Il Titolare del trattamento designa il Responsabile della protezione dei dati o Data Protection Officer (DPO) quando:

- il trattamento è effettuato da un organismo pubblico;
- le attività del Titolare consistono in trattamenti che richiedono il monitoraggio sistematico;
- le attività del Titolare consistono nel trattamento su larga scala di categorie particolari di dati personali.

Il DPO deve essere in possesso di:

- un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- operare alle dipendenze del titolare del trattamento oppure sulla base di un contratto di servizio.

- Il DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.
- Il Titolare del trattamento mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.
- Il DPO svolge i seguenti compiti:
    - informa e fornisce consulenze al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
    - verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o dei Responsabili del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
    - fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
    - collabora con il Titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle Attività di trattamento, in collaborazione con l'Amministratore di Sistema e con le altre strutture competenti dell'Azienda, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;
    - assiste il Titolare, i Responsabili del trattamento e l'Amministratore di Sistema, nei rapporti con il Garante e nei rapporti con albi soggetti pubblici o privati, per quanto riguarda gli adempimenti derivanti dalla normativa in materia di riservatezza e protezione dei dati personali;
    - funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
    - cura l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'Azienda per l'applicazione della normativa vigente e del presente Regolamento;
    - funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva, di cui all'art. 21 del presente Regolamento.

I DATI TRATTATI

L'Azienda nell'esercizio delle sue funzioni istituzionali tratta, in modo anche automatizzato (totalmente o parzialmente), le seguenti categorie di dati relativi agli utenti, pazienti e congiunti dei pazienti e dipendenti:

- Dati personali comuni
- Dati sensibili e giudiziari
- Dati sensibili relativi alla salute
- Dati del personale dipendente e convenzionato dell'Azienda

Dato Personale: rappresenta qualunque informazione relativa a persona fisica, identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, anche

indirettamente, attraverso un'identificazione personale "come il nome, un numero di identificazione, dati relativi all'ubicazione, un'identificazione online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (art. 4 Regol. UE 2016/679)

Dato Sensibile: è il dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute dell'interessato.

Dato sensibile relativo alla salute: si intendono i dati personali riguardanti la salute fisica o mentale di una persona fisica, comprese le prestazioni di servizi di assistenza sanitaria, che rivelano informazioni relative allo stato di salute, (art. 4 Regol.UE 2016/679)

L'elenco è tassativamente formulato dal Codice e non può essere ampliato anche di fronte al carattere di riservatezza o di particolare rilevanza che un soggetto, o il senso comune, può attribuire ad altre tipologie di dati (es. reddito).

Dato Giudiziario: è il dato personale idoneo a rivelare i provvedimenti giudiziari penali ed amministrativi in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del c.p.p.

Il trattamento dei dati sensibili e, in particolar modo, dei dati sanitari e dei dati giudiziari, è sottoposto ad una tutela particolarmente rigorosa in base ai principi dettati dagli articoli 20, 21 e 22 del Codice sulla Privacy.

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

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 non eccedenti cioè limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("rivinco di minimizzazione dei dati");
- 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 (“esattezza")
- 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 stati trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati

esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
- 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 ("integrità e riservatezza");
- configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità ("rivincolo di necessità");

il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (art. 5 e 6, del Regolamento UE 2016/679):

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

IL TRATTAMENTO DEI DATI PERSONALI

Con l'espressione "trattamento", ai sensi dell'Art. 4 del GDPR, deve intendersi qualunque operazione o complesso di operazioni, compiuti con o senza l'ausilio di processi automatizzati applicati a dati personali o all'insieme di dati personali, concernenti:

- la raccolta dei dati;
- la registrazione dei dati, cioè il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
- l'organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, ecc.;
- la conservazione dei dati alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
- la consultazione;

- l'elaborazione, ovvero le operazioni che attribuiscono significato ai dati in relazione allo scopo per i quali essi sono stati raccolti;
- la modificazione dei dati registrati in relazione a variazioni o a nuove acquisizioni;
- la selezione, l'estrazione, e il raffronto, ipotesi specifiche che rientrano nell'ipotesi più generale dell'elaborazione;
- l'utilizzo;
- l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la comunicazione, ovvero la trasmissione dei dati ad uno o più soggetti determinati, in qualunque forma, anche mediante messa a disposizione o consultazione; non è comunicazione la trasmissione dei dati allo stesso interessato, al Responsabile e agli Incaricati del trattamento;
- la diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati (es.: pubblicazione all'albo, giornale, ecc.);
- la cancellazione;
- la distruzione.

Il trattamento dei dati personali è esercitabile solo da parte del Titolare del trattamento, dai responsabili e dagli incaricati. Non è consentito il trattamento da parte di persone non autorizzate.

Il trattamento dei dati personali raccolti direttamente dall'Azienda o pervenuti in via indiretta da altri soggetti è effettuato sia con strumenti elettronici che senza l'ausilio degli strumenti stessi.

Il trattamento di dati personali anche sensibili comunicati dall'interessato direttamente o eventualmente raccolti presso gli uffici dell'AOPC di Catanzaro (es. Presidi Ospedalieri, Centri Prenotazioni, ecc..) è effettuato solo previo consenso dello stesso e per le finalità di trattamento legate alle cure o alla ricerca scientifica e alla didattica che siano strettamente necessarie allo svolgimento delle attività istituzionali.

Il trattamento è effettuato nel rispetto degli articoli 18, 19, 20, 21 e 22 del Codice della Privacy.

Il trattamento si considera lecito nelle specifiche ipotesi disciplinate nell'art. 6, primo paragrafo del Regolamento UE 2016/679, come previsto all'art.13 punto h) del presente regolamento.

Il trattamento dei dati personali ordinari è effettuato dall'Azienda, in quanto soggetto pubblico ed è consentito solo per lo svolgimento delle funzioni istituzionali pertanto è finalizzato all'erogazione delle prestazioni sanitarie, allo svolgimento degli adempimenti amministrativi-contabili e alle attività di organizzazione e di controllo a supporto dell'erogazione delle prestazioni sanitarie, con particolare riguardo alle attività di:

- diagnostica strumentale e di laboratorio;
- ricovero ordinario e in day- hospital;
- prestazioni sanitarie a rilevanza sociale;
- attività o servizi socio-assistenziali su delega dei singoli enti locali;

- medicina legale;
- ricerca e sperimentazione, nonché elaborazione statistica, epidemiologica e sociologica;
- controllo della salute dei lavoratori che operano all'interno dell'Azienda.

L'azienda effettua, altresì, i trattamenti di dati personali previsti da norme legislative e regolamentari riguardanti:

- la gestione del personale dipendente, ivi comprese le procedure di assunzione;
- la gestione dei soggetti, che intrattengono rapporti giuridici con l'Azienda, diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno dell'Azienda stessa, ivi compresi gli specializzandi, gli allievi e i docenti di corsi, i tirocinanti, i volontari;
- la gestione dei rapporti con i consulenti, i fornitori per l'approvvigionamento di beni e di servizi nonché con le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione;
- la gestione dei rapporti con i soggetti accreditati o convenzionati;
- la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.

Il DPO provvede, in collaborazione con i Responsabili del Trattamento, al censimento e all'aggiornamento di tutti i trattamenti di dati personali effettuati.

È compito del Responsabile del trattamento dei dati effettuare la valutazione periodica della non eccedenza dei dati trattati.

Le modalità del trattamento sono indicate negli articoli 11, 14, 17 e 22 del Codice della Privacy.

Il trattamento di categorie particolari di dati personali viene effettuato nel pieno rispetto dell'art. 9 del Regolamento UE 2016/679.

La comunicazione dei dati comuni trattati dall'Azienda ai soggetti pubblici, esclusi gli enti pubblici economici, può avvenire solo nei casi previsti da norme di legge o di regolamento. In mancanza, la comunicazione può essere effettuata quando sia comunque necessaria per lo svolgimento di funzioni istituzionali, secondo le modalità previste dall'art. 19, comma 2, del Codice della Privacy e le eventuali specifiche determinazioni del Garante.

I dati comuni possono essere comunicati a soggetti privati o a enti pubblici economici solo se è consentito dalla norma di legge o regolamento.

I dati personali oggetto del trattamento devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
- raccolti e registrati per scopi determinati, espliciti e legittimi e in seguito trattati in modo che non sia incompatibile con tali finalità ("limitazione della finalità");

- adeguati, pertinenti e limitati a quanto necessario rispetto alla finalità per le quali sono stati trattati ("minimizzazione dei dati");
- esatti, e se necessario, aggiornati ("esattezza");
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti ("pertinenza, completezza");
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi per i quali sono stati raccolti;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure e tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dai danni accidentali ("integrità e riservatezza");

Il Titolare del trattamento è competente per il rispetto dei sopracitati principi e deve essere in grado di comprovarlo ("responsabilizzazione").

IL TRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI

L'Azienda, in quanto soggetto pubblico, può trattare i dati sensibili, che non siano di natura sanitaria, solo quando il trattamento è autorizzato da espressa disposizione di legge nella quale sono ivi specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e l'indicazione del perseguimento di finalità di rilevante interesse pubblico; fatto salvo quanto è previsto dal secondo comma dell'art. 20 del Codice della Privacy.

L'Azienda può trattare i dati sensibili e giudiziari indispensabili per lo svolgimento di attività istituzionali mediante il trattamento di dati anonimi.

Per il trattamento dei dati sensibili e giudiziari non deve essere richiesto il consenso dell'interessato, né l'eventuale acquisizione del consenso serve a sanare un trattamento effettuato senza i presupposti di legge.

In ogni ipotesi di trattamento dei dati sensibili e giudiziari occorre verificare, sia preliminarmente sia durante il trattamento, che i dati trattati siano indispensabili per svolgere le attività istituzionali e non sia possibile utilizzare solo dati anonimi.

Tale trattamento deve essere effettuato con modalità volte a prevenire la violazione dei diritti, delle libertà fondamentali e della dignità dell'interessato.

IL TRATTAMENTO DEI DATI SENSIBILI RELATIVI ALLA SALUTE

L'Azienda, in quanto organismo sanitario pubblico, può trattare i dati personali idonei a rivelare lo stato di salute con il consenso dell'interessato e sulla base dell'autorizzazione del Garante.

I due requisiti indicati possono essere richiesti alternativamente nelle seguenti ipotesi:

- se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato è possibile procedere con il solo consenso dello stesso, anche senza l'autorizzazione del Garante;

- se la finalità di tutela della salute o dell'incolumità fisica riguarda un terzo o la collettività è possibile procedere sulla base dell'autorizzazione del Garante, anche senza il consenso dell'interessato.

Il Garante ha emesso un provvedimento di autorizzazione a carattere generale per il trattamento dei dati sanitari. L'autorizzazione è soggetta a rinnovo periodico e rende superflua la richiesta di singoli provvedimenti autorizzati da parte dell'Azienda.

I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

TRATTAMENTO DEI DATI DEL PERSONALE DELL'AZIENDA (dipendente e convenzionato)

L'Azienda tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo, così come specificato dall'art. 112 del Codice.

Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'Azienda è predisposta apposita informativa.

Secondo la normativa vigente, l'Azienda adotta le massime cautele nel trattamento di informazioni personali del proprio dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica. Il trattamento dei dati sensibili del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali, e quando non si possa prescindere dall'utilizzo dei dati giudiziari e sensibili, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.

La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando, piuttosto, diciture generiche o codici numerici. Non sono infatti sostenibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile

L'Azienda, nel trattamento dei dati sensibili relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.

L'Azienda assolve agli obblighi di legge in materia di trasparenza della Pubblica Amministrazione con la pubblicazione sul sito istituzionale dei dati relativi al personale.

L'Azienda applica quanto previsto dalle Linee Guida in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico ("Delibera Garante privacy del 14/06/2007").

NOTIFICAZIONE

Nelle ipotesi previste dall'art. 37 del Codice sulla privacy deve essere fatta notifica al Garante privacy quando il trattamento dei dati riguarda:

- dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato;
- dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi;
- dati registrati in apposite banche di dati gestite con strumenti elettronici.

Il Garante può, con provvedimento, individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, tenendo conto delle relative modalità o della natura dei dati personali oggetto di trattamento. Il Garante può, con provvedimento analogo, sottrarre dall'obbligo di notificazione i trattamenti di cui al comma primo del presente articolo, qualora i relativi trattamenti non siano suscettibili di recare un pregiudizio ai diritti dell'interessato.

La notificazione del trattamento è effettuata dal Titolare del trattamento al Garante con le modalità di cui all’art. 38, secondo comma del Codice della Privacy.

La notificazione è presentata al Garante prima dell'inizio del trattamento ed una sola volta. Una nuova notificazione è richiesta anteriormente alla cessazione del trattamento o al mutamento di alcuni elementi oggetto del trattamento.

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

(art. 30 Regolamento UE 2016/679)

Il Titolare del trattamento e ciascun responsabile del trattamento devono istituire un registro, in forma scritta, delle attività di trattamento svolte sotto la propria responsabilità, che deve essere

continuamente aggiornato e messo a disposizione delle autorità di controllo. Per ciascun trattamento, indicato nel registro, deve corrispondere l'individuazione del responsabile. Tale registro contiene alcune informazioni:

- Il nome e i dati di contatto del Titolare del trattamento, del responsabile per la protezione dei dati, dei Responsabili esterni e degli incaricati;
- Le finalità del trattamento;
- Una descrizione delle categorie di interessati e delle categorie dei dati personali;
- Le categorie dei trattamenti effettuati;
- Le categorie di destinatari a cui i dati personali sono o saranno comunicati;
- L'indicazione delle cautele specifiche, a cui ciascun responsabile deve attendere in modo che siano appropriate rispetto ai trattamenti verso cui dovrà rispondere;
- Eventuale possibilità di trasferimenti di dati all'estero;
- Una descrizione generale delle misure di sicurezza generiche e specifiche così come disciplinate dalla normativa vigente in tema di sicurezza dei dati personali;
- Indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI Dati

(Regolamento UE 2016/679 art. 35)

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

Il titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il responsabile della protezione dei dati.

Prioritariamente deve essere definito dal Titolare del trattamento l'elenco delle tipologie di trattamenti soggette al requisito della valutazione d'impatto sulla protezione dei dati.

La valutazione deve contenere almeno:

- Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare 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, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente 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 del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

Il Titolare, prima di procedere al trattamento dei dati, consulta, per il tramite del Data Protection Officer, il Garante privacy qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adeguate.

INFORMATIVA

Il Responsabile del trattamento, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, avvalendosi del personale incaricato, l'informativa prevista nell'art 13 del Codice della Privacy.

Le modalità per fornire l'informativa l'interessato sono definite d'intesa tra il DPO e i Responsabili del Trattamento.

L'informativa è fornita per iscritto, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
- avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture dell'Azienda, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet dell'Azienda;
- apposita avvertenza inserita nei contratti o nelle lettere di affidamento al servizio del personale dipendente, del personale medico convenzionato, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, degli specializzandi, tirocinanti, dei volontari, ecc. Per quanto riguarda i soggetti che hanno già instaurato rapporti con l'Azienda, l'informativa è fornita nei tempi e nei modi che saranno concordati tra il DPO e i Responsabili del trattamento;
- resa in sede di pubblicazione dei bandi, con l'indicazione del responsabile del trattamento dei dati relativi alle procedure concorsuali, all'affidamento di lavori o gare di forniture di beni e di servizi.

L'informativa contiene:

- le finalità e le modalità del trattamento;
- l'indicazione della natura facoltativa del conferimento dei dati;
- le informazioni per la costituzione del dossier sanitario elettronico sulla base del consenso espresso dall'interessato e possibilità di oscuramento di alcuni dati dello stesso;
- l'indicazione dei soggetti titolari, responsabili e incaricati del trattamento;
- il trattamento dei dati in casi particolari;
- l'indicazione dei diritti dell'utente;

- l'ambito di comunicazione e diffusione dei dati;
- l’esercizio dei propri diritti al riguardo della modifica, integrazione, cancellazione, rettifica ed il diritto all’oblio.

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'Azienda/convenzionato

Nei bandi di gara è inserita la seguente formula di informativa: "Ai sensi del Decreto Legislativo n. 196 del 30.06.2003, i dati forniti dalle ditte saranno trattati dall'Azienda esclusivamente per le finalità connesse alla gara di cui al presente bando e per la successiva stipula e gestione del contratto".

Nei contratti, accordi o convenzioni è inserita la seguente formula di informativa: " Ai sensi del Decreto Legislativo n. 196 del 30.06.2003, i dati personali forniti saranno trattati esclusivamente per finalità di gestione del presente contratto. Il soggetto affidatario si impegna, nel trattamento dei dati personali effettuati in forza del rapporto contrattuale, all'osservanza delle norme del GDPR e del Regolamento aziendale.

Nei bandi di concorso pubblico è inserita la seguente formula di informativa:

"Ai sensi del Decreto Legislativo n. 196 del 30.06.2003, i dati personali, anche di natura sensibile o giudiziaria, forniti dai candidati per la partecipazione al concorso, saranno trattati esclusivamente per le finalità di gestione del medesimo e per l'eventuale assunzione in servizio ovvero per la gestione del rapporto di lavoro".

Nelle segnalazioni di disservizio inviate all'Ufficio Relazioni con il Pubblico è inserita la seguente formula di informativa: "Ai sensi del Decreto Legislativo n. 196 del 30.06.2003, i dati personali forniti saranno trattato esclusivamente per la gestione della presente segnalazione".

In tutte le altre ipotesi di trattamento dati dovrà essere utilizzata una formula di informativa analoga alla seguente ed eventualmente adattata alla fattispecie particolare; "Ai sensi del Decreto Legislativo n. 196 del 30.06.2003, i dati personali, anche di natura sensibile o giudiziaria, forniti in relazione alla presente procedura, saranno trattati esclusivamente per le finalità di gestione della medesima e dell'eventuale rapporto contrattuale ad essa conseguente".

CONSENSO AL TRATTAMENTO DEI DATI

Nei trattamenti dei dati personali o sensibili, effettuati per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato, l'Azienda organizza modalità atte a facilitare l'espressione del consenso da parte dell'interessato, secondo le indicazioni contenute negli articoli 81 e 82 del Codice della Privacy. Quando il trattamento riguarda dati sensibili deve essere reso in forma scritta.

In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, successivamente alla prestazione, da parte

di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.

Il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione dell'apposito modulo allegato al presente regolamento previa consegna e presa d'atto dell'apposita informativa . La manifestazione del consenso, ad opera dell'interessato, verrà resa al momento del primo accesso o qualunque altro accesso alle prestazioni sanitarie e sarà valido ed efficace fino alla revoca dello stesso o, per i minorenni fino al compimento del diciottesimo anno di età. Il consenso è validamente prestato al ricorrere di determinate caratteristiche, ovvero sia reso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13 del Codice della Privacy. Il consenso viene registrato nell'anagrafe informatica secondo le tipologie prestate.

Il consenso è libero, autonomo e distinto per le seguenti casistiche:

a) consenso generale al trattamento dei dati personali e sensibili;

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento, con la stessa facilità con cui è accordato. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

Il consenso prestato è valido in relazione alla totalità dei trattamenti effettuati nell'ambito dell'AOPC di Catanzaro.

Il consenso ai sensi della normativa sulla privacy non deve essere confuso con il "consenso informato" necessario per poter sottoporre un paziente ad un determinato trattamento sanitario. In quest'ultima ipotesi, infatti, il paziente viene informato sul percorso diagnostico-terapeutico che gli viene proposto per poter decidere se sottoporsi a determinati accertamenti diagnostici, o trattamenti terapeutici, farmacologici o chirurgici.

COMUNICAZIONE DI DATI SANITARI ALL'INTERESSATO

I dati personali idonei a rivelare lo stato di salute possono essere resi noti

- all'interessato;
- ad un soggetto appositamente delegato per iscritto dall'interessato.

In caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato:

- a chi esercita legalmente la potestà; in caso di minore è necessario acquisire nuovamente il consenso del diretto interessato al raggiungimento della maggiore età;
- a un prossimo congiunto, a un familiare, a un convivente o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato.

COMUNICAZIONI E NOTIZIE SULLO STATO DI SALUTE DEGLI UTENTI

Le comunicazioni e le informazioni sulle specifiche patologie dell'interessato possono essere rese a quest'ultimo solo per il tramite del medico dell'Azienda competente in relazione ai provvedimenti organizzativi aziendali, ovvero per il tramite del medico di fiducia dell'interessato da lui designato o del medico che ha prescritto il ricovero o gli accertamenti.

Il Responsabile del trattamento dei dati personali può autorizzare per iscritto gli esercenti le professioni sanitarie diversi dai medici che, nell'esercizio dei propri compiti, intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato. L'autorizzazione è disposta in sede di designazione dei predetti esercenti quali incaricati al trattamento dei dati e ne individua i limiti, le modalità e le cautele ai sensi dell'art. 84 del Codice sulla Privacy.

Nel caso l'interessato si trovi in stato di impossibilità fisica, di incapacità di agire, di incapacità di intendere e di volere, le comunicazioni e le informazioni di cui ai commi 1 e 2 sono rese a chi dimostri, anche mediante autocertificazione resa ai sensi dell'art. 46 del D.P.R. 28.12.2000 n. 445, di esercitare legalmente la potestà ovvero di essere un prossimo congiunto, un familiare, un convivente, o, in loro assenza, il responsabile della struttura presso cui dimora.

Le informazioni di cui ai commi 1 e 2 possono essere rese anche a familiari dell'interessato o a terzi, durante il suo ricovero o in sede di pronto soccorso, soltanto previo consenso scritto dell'interessato stesso, da acquisire preventivamente con apposito modello.

Le cartelle cliniche, i referti di pronto soccorso, i referti concernenti le prestazioni diagnostiche, le relazioni e le schede sanitarie, le certificazioni rilasciate da organismi sanitari, nonché qualsiasi altro documento contenente dati personali idonei a rivelare lo stato di salute, sottoscritti dalle persone competenti, in relazione alla vigente normativa e agli atti di organizzazione aziendale, e redatti in forma intelligibile per l'interessato, sono consegnati in busta chiusa al medesimo ovvero a persona da lui delegata per iscritto, munita di documento di riconoscimento proprio e, anche in fotocopia, del delegante, dei quali dovranno essere annotati gli estremi.

ACCESSO ALLE LISTE DI ATTESA

La normativa vigente prevede che l'interessato ha il diritto di conoscere, anche tramite un proprio delegato da identificarsi, il numero di posizione che occupa nelle liste delle prestazioni ambulatoriali, di diagnostica strumentale e di laboratorio, dei ricoveri ospedalieri e nelle altre liste di attesa, ma non può essere messo a conoscenza dei nominativi delle persone che lo precedono o che lo seguono nell'elenco.

Fuori dei casi di cui al primo comma, le informazioni sulle prenotazioni e sui relativi tempi di attesa sono fornite ai soggetti che vi abbiano interesse, a norma della legge 7 Agosto 1990,n. 241, con la salvaguardia del diritto alla riservatezza delle persone.

PROCEDURE ORGANIZZATIVE A TUTELA DELLA RISERVATEZZA IN AMBIENTE SANITARIO

Presso tutti i presidi dell'Azienda, a cura del dirigente della struttura, sono adottate procedure, quali l'adozione di opportuna segnaletica per delimitare le distanze di cortesia, atte a garantire la riservatezza degli utenti in occasione di richiesta o fruizione di prestazioni sanitarie (prenotazioni, esami diagnostici, visite mediche, certificazioni, etc.) o amministrative (rimborsi, indennità, ecc.).

Nelle sale di attesa i pazienti non possono essere chiamati per nome.

I dirigenti delle strutture nonché i responsabili dei trattamenti sono tenuti ad adottare idonee misure atte a garantire che le informazioni sanitarie personali rese agli utenti verbalmente o tramite supporto cartaceo (documenti sanitari), non siano accessibili o percepibili da parte di terzi non espressamente autorizzati dagli interessati.

Le strutture ospedaliere possono fornire informazioni sui degenti, anche tramite il centralino telefonico, relativamente alla loro presenza in ospedale e sulla loro

collocazione all'interno della struttura, previo consenso dell'interessato che dovrà indicare anche i soggetti ai quali possono essere date le informazioni.

Non possono essere esposti al pubblico, nei reparti o in altri locali, i nominativi dei pazienti ricoverati.

PUBBLICITÀ DEGLI ATTI E DIRITTO ALLA RISERVATEZZA

Salva diversa disposizione di legge, l'Azienda garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo online o di altri atti, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati.

Laddove documenti e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati.

Non è consentita la diffusione online di dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità, handicap fisici e/o psichici.

Nel caso in cui un documento, soggetto a pubblicazione, riporti le informazioni di carattere sensibile o giudiziario dell'interessato, questo deve essere anonimizzato attraverso l'oscuramento totale del nominativo e delle altre informazioni.

I dati sensibili e giudiziari sono sottratti all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo.

Gli atti aziendali di AOPC di Catanzaro sono pubblicati nell'albo pretorio del sito internet istituzionale rispettando le disposizioni normative in materia.

L'Azienda applica in materia le disposizioni previste dal provvedimento del Garante sulla Privacy "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" del 15 maggio 2014.

DIRITTO DI ACCESSO ALLA DOCUMENTAZIONE E RISERVATEZZA

Fatti salvi gli atti sottratti all'accesso a norma di legge o di regolamento, l'Azienda garantisce il diritto di accesso alla documentazione amministrativa, nel rispetto dei limiti relativi alla tutela degli interessi giuridicamente rilevanti nei limiti in cui sia strettamente indispensabile, nonché nell'esercizio dello svolgimento delle investigazioni difensive di cui alla legge 7 Dicembre 2000, n.397.

L'istanza di acceso può essere negata per evitare un pregiudizio concreto alla protezione dei dati personali. Il limite riguarda solo alcuni dati o parti del documento richiesto, mentre deve essere consentito l'accesso agli altri dati che non comportano alcun pregiudizio per l'interessato. I limiti all'accesso si applicano unicamente per il periodo nel quale la protezione è giustificata in relazione alla natura del dato.

Nel caso in cui l'istanza avanzata dal richiedente riguardi una documentazione contenete dati riservati comuni o sensibili di terzi, l'accesso è limitato alla sola visione dei dati la cui conoscenza sia necessaria per curare o difendere un proprio interesse giuridico, nel rispetto dei principi di pertinenza e di non eccedenza dei dati da visionare rispetto alle finalità per le quali è consentito l'accesso.

Qualora l'istanza di accesso riguardi documenti contenenti dati idonei a rivelare lo stato di salute o la vita sessuale di un terzo, l'accesso è consentito solo se la situazione giuridicamente rilevante che si intende tutelare in sede giudiziaria sia di rango almeno pari ai diritti del terzo, ovvero consiste in un diritto della personalità o altro diritto o libertà fondamentale e inviolabile, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso.

L'Azienda valuterà caso per caso la possibilità di accedere ai documenti da parte di terzi e qualora autorizzi l'accesso dovrà effettuare una attenta valutazione su quali informazioni debbano essere comunicate e quali invece siano eccedenti, rispetto allo scopo perseguito con l'accesso.

RINVIO A PREVISIONI DI NORMATIVA SPECIALE

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

- dall'art. 5, della Legge 5 giugno 1990, n. 135, come modificato dall'art. 178 del Codice, secondo cui la rivelazione statistica della infezione da HIV deve essere effettuata con modalità che non consentano l'identificazione della persona;
- dall'art. 11 della Legge 22 maggio 1978, n. 194, il quale dispone che l'ente ospedaliero, la casa di cura o il poliambulatorio nei quali è effettuato un intervento di interruzione di gravidanza devono inviare alla Regione una dichiarazione che non faccia menzione dell'identità della donna;
- dall'art. 734-bis del Codice Penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano altresì fermi gli obblighi di legge che vietano la rivelazione, senza giusta causa, e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici previsti, in particolare, dal Codice di deontologia medica adottato dalla Federazione nazionale degli ordini dei medici chirurghi e dagli odontoiatri.

CARTELLA CLINICA

Il Responsabile dell'Unità operativa che ha in carico il paziente risponde della regolarità nella redazione della Cartella clinica; essa deve essere conclusa con la diagnosi di dimissione e firmata dal Responsabile sopracitato o da un suo collaboratore a ciò appositamente delegato. La cartella clinica è un atto pubblico di fede privilegiata che deve essere conservata per un periodo di tempo illimitato.

La compilazione delle cartelle cliniche deve garantire la comprensibilità dei dati in modo che siano distinti i dati relativi al Paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

di far valere o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato, cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile; di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Nel caso di decesso dell'interessato il richiedente può accedere ai dati personali presenti nella cartella clinica qualora dimostri di agire a tutela del deceduto o per ragioni familiari meritevoli di protezione.

L'accesso è normalmente consentito agli eredi che auto certifichino il loro status di eredi.

Il rilascio della cartella clinica o di referti clinici o di altra documentazione sanitaria è inoltre consentito a soggetti non intestatari della documentazione stessa nei seguenti casi:

- richiesta da parte degli organi giudiziari;

- richiesta del Direttore medico di Presidio ospedaliero e del legale rappresentante di altro Ospedale e Casa di cura diversi da quelli presso i quali la documentazione sanitaria è conservata, qualora il paziente si trovi in esso ricoverato e sia necessario acquisire dati utili al trattamento dello stato morboso in atto, quindi per finalità di tutela della salute e dell'incolumità fisica del paziente, dietro richiesta su carta intestata con firma del medico di reparto richiedente che dichiari anche generalità di chi ritira la documentazione;
- richiesta da parte del Consulente Tecnico d'Ufficio, previa esibizione dell'atto di nomina e di autorizzazione del giudice;
- I.N.A.I.L., nei casi di infortunio o di malattia professionale occorso ad un assicurato, con delega sottoscritta dall'assistito (artt. 94 e 95 del D.P.R. 3.6.1965 n. 1124; art. 5 all. A al D.M. 15.3.1991);
- I.N.P.S., con delega sottoscritta dall'assistito, nei casi in cui competano a questo le spese di spedalità per i pazienti dipendenti da aziende private (artt. 17 e 18 del D.P.R. n. 2316 del 1934);
- Prefetture per spese di ricovero ospedaliero urgente di cittadini stranieri che dichiarino lo stato di indigenza, per i quali si richiede il rimborso del costo del ricovero direttamente all'Autorità Prefettizia (Legge 17.7.1890 n. 6972; R.D. n. 99 del 5.2.1891, art. 114);
- richiesta da parte di persona esercente la potestà genitoriale, previa autocertificazione del relativo status;
- richiesta del medico di base, che ha in cura il paziente, con esplicitazione della indispensabilità di accedere a tali documenti per la tutela dell'incolumità fisica e della salute del paziente e mediante contestuale presentazione di documentazione idonea a dimostrare il consenso scritto dell'interessato;
- richiesta da parte del curatore d e 1 la persona inabilitata, previa esibizione di documentazione probatoria e dichiarazione sostitutiva dell'atto di notorietà da cui risulti il relativo status;
- dall'amministratore di sostegno previa esibizione della copia del decreto di nomina del Giudice Tutelare che certifichi il relativo status.

La cartella clinica e la documentazione socio sanitaria possono essere consultate dal personale medico dell'Azienda, qualificato quale soggetto "Incaricato" o "Responsabile", ai sensi dell'art. 30 del Codice sulla Privacy, per finalità diagnostico-terapeutiche.

La consultazione delle cartelle cliniche per finalità di ricerca scientifica o statistica può essere effettuata sulla base di un atto motivato che ne giustifichi le finalità e deve essere autorizzata dalla Direzione sanitaria dell'Azienda. In questi casi i dati dovranno essere resi anonimi o comunicati in forma aggregata con modalità che rendono non identificabili i soggetti cui si riferiscono.

RICOVERO IN OSPEDALE

È possibile, in via generale, fornire ai parenti e conoscenti, che ne facciano richiesta, informazioni sulla presenza nelle strutture sanitarie, quali ricoverati, dei pazienti.

Soltanto nei casi in cui il paziente manifesti una volontà espressa di rifiuto alla comunicazione risulta necessario escludere ogni informazione sul ricovero.

Al momento del ricovero presso una struttura ospedaliera viene consegnato e fatto sottoscrivere all'interessato un apposito modulo che gli consenta di manifestare:

- l'eventuale rifiuto alla possibilità di comunicare ad altri soggetti la presenza nel reparto;
- il consenso alla comunicazione dei dati sanitari (e cioè delle condizioni di salute) dell'interessato a selezionate categorie di familiari o ad altre persone specificatamente indicate.

RITIRO DEI REFERTI O ALTRA DOCUMENTAZIONE CONTENENTE DATI SANITARI

Il ritiro dei referti o altra documentazione contenente dati sullo stato di salute può essere effettuato:

- dal diretto interessato;
- da chi esercita la tutela, in caso di minore o di interdetto;
- dal delegato dell'interessato munito di delega, documento proprio e documento del delegante (anche in copia).

La consegna dei documenti deve essere effettuata in busta chiusa.

Non è possibile la comunicazione per via telefonica dei risultati delle analisi salvo situazioni di assoluta necessità e urgenza a tutela dell'incolumità fisica dell'interessato.

VIDEOSORVEGLIANZA

Si rinvia a specifico Regolamento allegato al presente e aggiornato a Dicembre 2016.

DIRITTI DELL'INTERESSATO

L'interessato è il soggetto, persona fisica, alla quale si riferiscono i dati oggetto del trattamento.

L'Azienda attua tutte le misure necessarie a facilitare l'esercizio dei diritti dell'interessato ai sensi dell'art. 7 del Codice e degli artt. 12-22 del Regolamento UE 2016/679.

A tal fine il Codice sulla privacy e la normativa europea sopracitata prevedono che l'interessato ha diritto di ottenere dal titolare del trattamento:

- conferma dell'esistenza o meno di dati personali che lo riguardano e se sia in corso o meno un trattamento degli stessi e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

  • origine dei dati;

  • finalità e modalità del trattamento;

  • la logica applicata e i criteri utilizzati nell'elaborazione elettronica dei dati;

  • gli estremi identificativi del Titolare e del Responsabile del trattamento;

  • i soggetti e le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza;

• periodo di conservazione dei dati personali previsto, o se non esplicitamente indicato, i criteri utilizzati per la determinazione di tale periodo.

- ottenere una comunicazione dei dati, oggetto del trattamento, che sia concisa, trasparente, intelligibile, e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate ai minori;
- richiedere la rettifica/aggiornamento dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo; l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
- ottenere la cancellazione (diritto all'oblio) dei dati personali che lo riguardano, se trattati in violazione di legge, senza ingiustificato ritardo o quando ricorra uno dei motivi di cui all'art. 17 del Regolamento UE 2016/679. Nel caso in cui, il titolare del trattamento abbia reso pubblici i dati dell'interessato ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure e tecniche ragionevoli per informare i titolari del trattamento, a cui sono pervenuti i dati personali, della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Tale diritto trova alcune limitazioni nell'art. 17, terzo paragrafo, del Regolamento UE 2016/679;
- ottenere la trasformazione in forma anonima o il blocco se trattati in violazione di legge;
- ottenere attestazione che tali interventi sui dati sono stati portati a conoscenza (anche per il contenuto) di coloro ai quali i dati sono stati comunicati;
- Di ottenere la limitazione del trattamento dei dati personali quando ricorre una delle ipotesi previste nell'art. 18 alla lett. a), b), c), d) del Regolamento UE 2016/679. A seguito dell'esercizio, da parte dell'interessato, del diritto di limitazione del trattamento i dati personali sono trattati, salvo che per la conservazione, solo con il consenso dello stesso o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante;
- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento, se tecnicamente fattibile e senza limitazioni qualora: il trattamento si basi sul consenso o contratto dell'interessato e il trattamento sia automatizzato.
- Il diritto alla portabilità dei dati è derogabile nel caso in cui il trattamento dei dati sia necessario per l'esecuzione di un pubblico interesse o sia connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale diritto non deve ledere i diritti e le libertà altri;
- proporre opposizione al trattamento dei dati. A seguito dell'esercizio del diritto di opposizione, da parte dell'interessato, il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sui diritti, interessi e libertà dell'interessato;
- ottenere una copia dei dati personali oggetto di trattamento. Qualora l'interessato faccia richiesta di ottenere più copie, il Titolare del trattamento può attribuire un contributo spese ragionevole tenendo conto dei costi amministrativi. Se la richiesta dell'interessato perviene con mezzi elettronici, salvo diversa indicazione dell'interessato, le informazioni saranno rese

in un formato elettronico di uso comune. Il diritto dell'interessato, ad ottenere una copia dei dati personali che lo riguardano, viene contemperato con il diritto di non ledere i diritti e le libertà altrui.

MODALITÀ DI ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Per i diritti dell'interessato in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni previste dagli articoli 7,8, 9 e 10 del Codice.

La richiesta per l'esercizio dei diritti di cui all'art. 38 del presente Regolamento può essere fatta pervenire:

Direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso (es. la conoscenza personale);

Tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;

Tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;

In caso di persone decedute, tali diritti possono essere esercitati da che ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;

Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai relativi statuti od ordinamenti.

L'interessato può presentare o inviare la richiesta di esercizio dei diritti

Al Titolare o Responsabile del trattamento, che conserva e gestisce i dati personali dell'interessato;

All'Ufficio protocollo generale dell'Azienda o all'Ufficio per le relazioni con il pubblico, che ne curano l'inoltro al Titolare del trattamento.

La richiesta per l'esercizio dei diritti, di cui al primo comma, può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non ai dati relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano. Il responsabile del trattamento autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso.

I soggetti competenti alla valutazione dell'istanza sono: il Titolare e/o Responsabile dei dati di cui si richiede l'accesso; il DPO; il Responsabile SIA (Amministratore di sistema) i quali congiuntamente decidono sull'ammissibilità della richiesta d'accesso e sulle modalità per consegnare/limitare/cancellare (se l'interessato esercita tale diritto con motivata richiesta).

All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa. I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.

L'accesso dell'interessato ai propri dati personali può essere differito, a norma dell'art. 7 del D.P.R. 27 Giugno 1992,n.352, limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza dell'Azienda. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.

INDAGINI DIFENSIVE

Nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art. 391-quater del Codice di Procedura Penale, ha facoltà di svolgere

investigazioni per ricercare ed individuare elementi di prova a favore del proprio assistito.

Ai fini di tali indagini, il difensore può chiedere documenti in possesso dell'Azienda (e può estrarne copia a proprie spese) anche se contengono dati personali di un terzo interessato.

Il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'interessato, e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile.

Si fa rinvio al Regolamento aziendale sul diritto di accesso.

FORMAZIONE DEL PERSONALE

L'Azienda organizza, nell'ambito dell'istituito di formazione continua e obbligatoria del personale, interventi di formazione e aggiornamento in materia di tutela della riservatezza e protezione dei dati personali, finalizzati alla conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni ai dati stessi.

MISURE DI SICUREZZA

L'Azienda nel trattamento dei dati personali garantisce l'applicazione di idonee e preventive misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

Secondo la normativa vigente in materia, il Titolare del trattamento e il Responsabile del trattamento mettono in atto misure e tecniche organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono:

- la pseudominizzazione e la cifratura dei dati personali trattati;

- procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Titolare e il Responsabile del trattamento fanno sì che chiunque agisce sotto la loro autorità e ha accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare.

Per quanto attiene al trattamento dei dati personali effettuato con strumenti elettronici e non, l'Azienda applica le misure minime disciplinate dagli articoli da 33 a 36 del Codice sulla privacy

RESPONSABILITÀ IN CASO DI VIOLAZIONE DELLE DISPOSIZIONI IN MATERIA DI PRIVACY.

COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI (art. 33 e 34 Regolamento UE 2016/679 DATA BREACH)

La comunicazione dell'eventuale avvenuta violazione dei dati personali (DATA BREACH) deve, immediatamente, essere effettuata al DPO, non appena si è verificato l'evento, senza ingiustificato ritardo, in quanto lo stesso evento dovrà essere annotato sul Registro del Data Breach ed essere informato, entro 72 ore, il Garante dell'avvenuta violazione.

La notifica deve:

- Descrivere la natura della violazione dei dati personali;
- Descrivere le probabili conseguenze della violazione;
- Descrivere le misure adottate o di cui si propone l'adozione.

Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato, senza ingiustificato ritardo. La comunicazione all'interessato descrive, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali. Non è richiesta la comunicazione qualora ricorra una delle seguenti condizioni:

Il Titolare del trattamento ha messo in atto, preventivamente, delle misure e tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto di violazione, (ad esempio la cifratura);

Il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà dell'interessato;

La comunicazione richiederebbe sforzi sproporzionati; in tal caso si procede a una comunicazione pubblica o a una misura simile tramite la quale gli interessati sono informati con analoga efficacia.

NORMA FINALE

Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni ed integrazioni),i provvedimenti specifici del Garante per la protezione dei dati personali e il Regolamento europeo 2016/679 del 27.04.2016.

Il presente Regolamento sarà aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.

ALLEGATO 1

MODULO PER CONSENSO ALLA COMUNICAZIONE DEI DATI SANITARI IN REGIME DI RICOVERO
(artt. 76 e 83 D. Lgs. 196/03- Codice sulla Privacy)

Io sottoscritto/a _____

Nato a_____il _____

E residente in_____in via _____

Tel_____Mail _____

In qualità di [barrare la casella di interesse):

☐ Genitore/esercente la potestà per il minore	Convivente ☐
	prossimo congiunto familiare ☐
☐ Esercente la potestà Prossimo congiunto	

Considerato lo stato di [barrare la casella di interesse):

☐ Minore età l'impossibilità fisica	☐ incapacità di agire incapacità di intendere e volere

Di (inserire i dati dell'interessato, per cui si fa la dichiarazione, nel riquadro sottostante)

NOME	COGNOME
_____	_____

DICHIARO

Di aver ricevuto e compreso l'informativa per il trattamento dei dati sanitari, fornita ai sensi dell'art. 13 del Codice sulla privacy, e di aver espresso il mio consenso al trattamento dei miei dati sanitari o per conto dell'interessato sopra indicato.

E (barrare la casella di interesse):

☐ AUTORIZZO

La COMUNICAZIONE DEI DATI RELATIVI AL MIO STATO DI SALUTE O DELL'INTERESSATO A:

☐ figli ☐ coniuge ☐ fratelli/sorelle ☐ genitori ☐ famigliari in genere

Nato/a il

Residente in ..... via

Ricoverato presso il Reparto di

Solo se Lei desidera che non siano date informazioni sulla sua PRESENZA o dell'interessato in Ospedale, con indicazione del reparto di degenza, esprima la volontà espressa di rifiuto

☐ Non autorizzo

La COMUNICAZIONE A TERZI DELLA MIA PRESENZA 0 DELL'INTERESSATO come degente presso questo reparto del Presidio Ospedaliero.

Luogo e data Firma

ALLEGATO 2

c/o Azienda Ospedaliera “Pugliese-Ciaccio”

Via Vinicio Cortese, 25

88100 CATANZARO (CZ)

Spett.le

Dr

LETTERA DI INCARICO

Responsabile del trattamento dei dati personali

D. Lgs. 30.6.2003 n. 196

All- B - Disciplinare Tecnico in materia di misure di sicurezza per la protezione dei dati personali

OGGETTO: Lettera di Incarico al Responsabile del Trattamento dei dati.

Unità Operativa

In qualità di "Titolare dei Trattamento" dei dati personali, IL Direttore Generale pro-tempore, conformemente a quanto stabilito dal D. Lgs. 30.6.2003 n. 196

AFFIDA A

Dr._____, la mansione di Responsabile del Trattamento dei dati, con l'incarico di realizzare il sistema di sicurezza per la Privacy della succitata Unità Operativa, in base alle scelte e regole contenute nell'Allegato "DELEGA AL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI" in calce riportata.

Ai fini suddetti il RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI dovrà, nella propria Unità Organizzativa, incaricare al trattamento dei dati ogni singolo dipendente (con lettera d'Incarico allegata alla presente) ad essa afferente; nonché curare la custodia delle Password di accesso degli incaricati ad ogni singola postazione afferente alla propria Unità Organizzativa o, eventualmente, individuare un dipendente, appartenente all'Unità Operativa da lui diretta, a cui demandare, per iscritto, tale compito. A tal fine si ricorda che la Password deve essere composta da almeno otto caratteri alfanumerici con l'aggiunta di caratteri speciali e dovrà essere sostituita ogni tre mesi se il trattamento del dato è di natura sensibile e/o giudiziario, ogni sei mesi se di natura ordinario. La custodia dovrà essere annotata su di un Registro creato ad hoc al fine di dimostrare, in casi di controllo, la relativa evidenza oggettiva della Policy. Riepilogando, la Password di Windows dovrà essere trascritta su di un foglio bianco con l'indicazione del soggetto, inserita in una busta, riportante all'esterno solo il nominativo dell'dipendente, e, previa chiusura, consegnata al Custode delle password dell'Unità Operativa.

In previsione del dell'avvio del nuovo GDPR (UE 679/2016), che entrerà in vigore a far data del 25 maggio 2018, si ritiene anche di dover anticipare quanto indicato nell'art. 35 del GDPR, attuando maggiori misure di sicurezza prevedendo una password (sempre di otto caratteri alfanumerici con caratteri speciali) anche sui software utilizzati presso ogni singola postazione delle Unità Operative (semplici e/o complesse).

Al riguardo della protezione dei dati diventa importante l'art. 25 del regolamento europeo, quindi, si intenderà una nuova Policy (Privacy by Default e Privacy by Design) a livello di analisi dei Rischi.

È fondamentale, quindi, dotarsi di un'Organizzazione interna all'Unità Operativa che sia di supporto al Titolare dei dati per il trattamento degli stessi in totale accordo col nuovo Regolamento europeo UE 2016/679.

Il "Responsabile del Trattamento" dichiara di essere a conoscenza di quanto stabilito dal D. Lgs. 30.6.2003 n. 196 sulla privacy e dall'All. B al decreto stesso (Disciplinare Tecnico in materia di misure minime di sicurezza per la protezione dei dati) nonché del GDPR 679 del 2016 per l'adozione delle misure di sicurezza e si impegna ad attuare le norme in esso contenute.

La Formazione sul nuovo regolamento europeo ha avuto inizio nel 2017 ed si protrarrà per tutto il 2018 al fine di garantire un'adeguata consapevolezza di trattamento nonché comportamentale dei dati conferiti all'Azienda Ospedaliera.

Sarà compito del Responsabile del Trattamento dei dati assicurarsi che tuti i dipendenti afferenti la propria struttura abbiano preso parte ai corsi di formazione sul nuovo regolamento europeo UE 2016/679.

Il Titolare

_____

(Azienda Ospedaliera "Pugliese-Ciaccio")

Il Responsabile del trattamento per accettazione dell'incarico

_____

(Dr._____)

DELEGA AL RESPONSABILE del Trattamento dei dati personali PER LA SICUREZZA

TRATTAMENTO DEI DATI PERSONALI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento di dati personali, effettuato con strumenti diversi da quelli elettronici o comunque automatizzati, dovrà essere richiesta almeno l'osservanza delle seguenti modalità finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento, da parte degli incaricati, nelle operazioni di trattamento, degli atti e dei documenti contenenti dati personali:

- individuare gli incaricati al trattamento dei dati personali e predisporre la lista degli incaricati che potrà essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione. Per ogni incaricato definire l'ambito del trattamento consentito e i relativi profili di autorizzazione. Provvedere con cadenza almeno annuale all'aggiornamento della lista e dei conseguenti incarichi: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;

- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari saranno affidati per lo svolgimento dei relativi compiti, i medesimi atti e documenti dovranno essere controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e, al termine delle operazioni affidate, dovranno essere da questi restituiti;

- l'accesso agli archivi contenenti dati sensibili o giudiziari dovrà essere controllato. Qualora gli incaricati del trattamento di dati personali dovessero trattare documenti contenenti dati personali sensibili o giudiziari e per far ciò dovessero accedere all'archivio gli stessi dovranno aver cura di esibire la documentazione comprovante l'autorizzazione all'accesso e al trattamento. Nel caso in cui gli incaricati fossero ammessi, a qualunque titolo, dopo l'orario di chiusura, dovranno dare le loro generalità in quanto vi è l'obbligo di identificare e registrare coloro che accedono agli archivi stessi. Qualora gli archivi non fossero dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, gli incaricati dovranno richiedere preventivamente l'autorizzazione all'accesso.

TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI ELETTRONICI

Per il trattamento di dati personali, effettuato con strumenti elettronici, dovrà essere richiesta almeno l'osservanza delle modalità di seguito indicate.

Sistema di autenticazione informatica.

Individuare gli incaricati al trattamento dei dati personali e predisporre la lista degli incaricati che potrà essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione. Per ogni incaricato definire l'ambito del trattamento consentito e i relativi profili di autorizzazione. Provvedere con cadenza almeno annuale all'aggiornamento della lista e dei conseguenti incarichi: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Il trattamento di dati personali con strumenti elettronici deve essere consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Per le credenziali occorrerà osservare quanto disposto dal Disciplinare tecnico (All. B al D. Lgs. 30.6.2003 n. 196).

Ad ogni incaricato devono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

Dovranno essere impartite agli incaricati istruzioni per adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

Deve essere previsto che:

- le credenziali di autenticazione non utilizzate da almeno sei mesi dovranno essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;

- le credenziali dovranno essere disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Devono essere impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Per i casi in cui l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, saranno impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

Sistema di autorizzazione

Nei casi in cui, per gli incaricati, saranno individuati profili di autorizzazione di ambito diverso dovrà essere operativo un sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, dovrà essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Sarà cura del Responsabile del Trattamento assicurarsi, anche per mezzo di personale di sua fiducia e afferente all'Unità operativa, che ad ogni paziente/utente venga fatto firmare il modulo di consenso informato su come saranno trattati i dati di ogni interessato che si avvale dei servizi dell'Azienda, con l'esercizio dell'art. 7 del D. Lgs. 196/03. Il consenso sarà custodito in cartella

clinica se trattasi di consenso trattato nei reparti. Il consenso dovrà essere gestito con un'organizzazione di rito, con relativa conservazione, in altre strutture quali: accettazione, ticket, analisi generiche (prelievi, day hospital, ecc.).

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

I dati personali dovranno essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare ogni qualvolta vengano resi disponibili gli aggiornamenti.

Dovranno essere effettuati aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.

Dovranno essere impartite istruzioni organizzative e tecniche per il salvataggio dei dati, con ragionevole frequenza (inizialmente settimanalmente), soprattutto sui singoli PC che non siano collegati ad un Server.

In modo da assicurare la dovuta padronanza di tutti i dipendenti delle Policy del Disaster Recovery e della Business Continuity da regolamentare con l'Amministratore di Sistema aziendale e di concerto col DPO.

Il responsabile del Trattamento dei dati dovrà avviare una elevata collaborazione col DPO Aziendale che dovrà curare la tenuta di un Registro dei Trattamenti, gli adempimenti di data Breach e fungere da interfaccia con la Struttura Garante.

Il calcolo dei Rischi, attuato dal DPO, sarà effettuato in collaborazione con tutti i Responsabili del Trattamento in sinergia con l'art. 32 del regolamento europeo.

Periodicamente il DPO verificherà, con audit interni, il perfetto andamento delle Policy impartite redigendo dei verbali, da sottoporre al Direttore Generale, indicanti l'andamento delle direttive, con cadenza almeno bimestrale, che consentano una piena attuazione del GDPR.

Trimestralmente il DPO convocherà tutti i Responsabili del Trattamento al fine di rendere più performante le attività di trattamento. Ogni Incident di sicurezza dovrà essere reso noto all'intera struttura, per il tramite del DPO, per mezzo di comunicazioni ufficiali mirate alla minimizzazione del rischio.

Dovendo il Responsabile del Trattamento dei dati coordinare l'Organizzazione interna della propria Unità Operativa avrà l'onere di consegnare la Lettera d'incarico al trattamento dei dati personali ad

ogni singolo impiegato dell'AOPC facente parte della suddetta Unità Operativa, creando, così, l'Unità Organizzativa di Reparto.

All'uopo si allega un fac-simile di Lettera d'Incarico al trattamento dei dati personali.

Procedura organizzativa:

Occorrerà fare la fotocopia di tale lettera firmata dal Responsabile del Trattamento Direttore dell'Unità Operativa (organizzativa) e consegnarla ad ogni singolo dipendente afferente la struttura di riferimento.

Per comodità si allega anche un foglio contenente ogni singolo dipendente afferente l'Unità (si prega di comunicare tempestivamente al Referente Privacy e/o DPO ogni variazione intervenuta: trasferimenti da e verso la struttura, nuove assunzioni, pensionamenti, altro).

Una volta consegnata la lettera d'incarico al trattamento dei dati personali ad ogni singolo dipendente/incaricato, lo stesso dovrà firmare un elenco di evidenza oggettiva da cui si evinca che la lettera è stata consegnata nella data indicata.

La formazione del personale afferente l'Unità Organizzativa sarà a cura del Responsabile del Trattamento dei dati dell'Unità Operativa; il quale dovrà verificare che tutti i dipendenti che trattano dati presso tale Unità siano stati formati con l'obbligo di indicare al DPO i nominativi di chi ancora non abbia partecipato ai corsi che periodicamente vengono effettuati.

Non sarà ammessa nessuna deroga, in quanto, il trattamento dei dati è sub judice ad una formazione continua e nondimeno, con l'entrata in vigore del GDPR 679/2016, ad esporre l'intera Azienda Ospedaliera a Verifiche da parte del Garante Privacy in funzione anche del Data Breach.

ALLEGATO 3

c/o AOPC

Via Vinicio Cortese, 25

88100 CATANZARO (CZ)

Spett.le

LETTERA DI INCARICO

Per incaricato al trattamento dei dati personali

D. Lgs. 30.6.2003 n. 196 sulla privacy

All. B – Disciplinare Tecnico in materia di misure di sicurezza per la protezione dei dati

A: _____

OGGETTO: Lettera all'Incaricato per il trattamento dei dati dell'Unità Operativa di appartenenza.

La presente per comunicarLe che nell'esecuzione della sua attività lavorativa esegue trattamenti di dati personali e prende visione di documenti che contengono i dati stessi.

La normativa sulla Privacy (D. Lgs. 30.6.2003 n. 196) ha disposto che il personale che presta l'attività a favore del titolare può accedere ai dati personali se incaricato per iscritto di compiere le operazioni del trattamento dal titolare o dal responsabile e sempre che operi sotto la loro diretta autorità attenendosi alle istruzioni da questi impartite (Art.30 D. Lgs. 30.6.2003 n. 196).

Lo scrivente, quindi, in qualità di Titolare del Trattamento dei dati personali (oppure Responsabile del Trattamento dei dati personali), conformemente a quanto stabilito dal D. Lgs. 30.6.2003 n. 196 conferma che nello svolgimento della sua attività potrà trattare:

i dati personali contenuti nei documenti che deve utilizzare nello svolgimento delle attività nell'unità organizzativa ad essa afferente e ad accedere ai relativi archivi;

I dati personali di cui all'area suddetta contenuti in archivi e in strumenti elettronici utilizzando gli strumenti stessi;Nell'effettuare il trattamento dei dati personali devono essere soddisfatti i principi contenuti nell'art. 11 del D. Lgs. 196/03; infatti, i dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi, devono essere esatti e, se necessario, aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati e la loro conservazione nella forma che consenta l'identificazione dell'interessato deve avvenire per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Nello svolgimento delle sue mansioni voglia adottare idonee misure di custodia e di controllo ed in genere qualunque accorgimento che consenta di ridurre al minimo i rischi di distruzione o perdita, anche accidentale di dei dati stessi e che consenta di ridurre al minimo i rischi di accesso non

autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta e voglia osservare le procedure appositamente approntate per evitare quanto detto.

Precisiamo che dovrà seguire le particolari regole di sicurezza specificamente previste per la protezione contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale (antiVirus, antiWorm, protezione da programmi maligni in genere), per l'aggiornamento dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti per curare, almeno settimanalmente, il salvataggio dei dati seguendo le istruzioni organizzative e tecniche che abbiamo impartito con appositi incarichi (si veda l'Allegato REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI).

Le ricordiamo che il Disciplinare Tecnico in materia di misure minime di sicurezza (All. B al D. Lgs. 30.6.2003 n. 196), prevede particolari regole alle quali ogni incaricato dovrà attenersi nel trattamento dei dati personali medesimi; regole che vengono riportate nel seguente Allegato REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI e che dovranno da Lei essere osservate.

Il Designante – Responsabile del trattamento

_____

IL RESPONSABILE DEL TRATTAMENTO dell'Unità Operativa

L'incaricato del Trattamento dichiara di essere a conoscenza di quanto stabilito dall'All. B - Disciplinare Tecnico in materia di misure minime di sicurezza e si impegna, nel trattamento dei dati personali ai quali è stato autorizzato ad accedere ad attenersi alle regole qui indicate comprese quelle di cui all'Allegato REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI.

L'incaricato

(per accettazione delle regole qui contenute)

_____

ALLEGATO 4

REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI

TRATTAMENTO DEI DATI PERSONALI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento di dati personali, effettuato con strumenti diversi da quelli elettronici o comunque automatizzati, dovrà essere richiesta almeno l'osservanza delle seguenti modalità finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento, da parte degli incaricati, nelle operazioni di trattamento, degli atti e dei documenti contenenti dati personali:

- individuare gli incaricati al trattamento dei dati personali e predisporre la lista degli incaricati che potrà essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione. Per ogni incaricato definire l'ambito del trattamento consentito e i relativi profili di autorizzazione. Provvedere con cadenza almeno annuale all'aggiornamento della lista e dei conseguenti incarichi: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;

- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari saranno affidati per lo svolgimento dei relativi compiti, i medesimi atti e documenti dovranno essere controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e, al termine delle operazioni affidate, dovranno essere da questi restituiti;

- l'accesso agli archivi contenenti dati sensibili o giudiziari dovrà essere controllato. Qualora gli incaricati del trattamento di dati personali dovessero trattare documenti contenenti dati personali sensibili o giudiziari e per far ciò dovessero accedere all'archivio gli stessi dovranno aver cura di esibire la documentazione comprovante l'autorizzazione all'accesso e al trattamento. Nel caso in cui gli incaricati fossero ammessi, a qualunque titolo, dopo l'orario di chiusura, dovranno dare le loro generalità in quanto vi è l'obbligo di identificare e registrare coloro che accedono agli archivi stessi. Qualora gli archivi non fossero dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, gli incaricati dovranno richiedere preventivamente l'autorizzazione all'accesso.

TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI ELETTRONICI

Per il trattamento di dati personali, effettuato con strumenti elettronici, dovrà essere richiesta almeno l'osservanza delle modalità di seguito indicate.

Sistema di autenticazione informatica.

Individuare gli incaricati al trattamento dei dati personali e predisporre la lista degli incaricati che potrà essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione. Per ogni incaricato definire l'ambito del trattamento consentito e i relativi profili di autorizzazione. Provvedere con cadenza almeno annuale all'aggiornamento della lista e dei conseguenti incarichi: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Il trattamento di dati personali con strumenti elettronici deve essere consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Per le credenziali occorrerà osservare quanto disposto dal Disciplinare tecnico (All. B al D. Lgs. 30.6.2003 n. 196).

Ad ogni incaricato devono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

Dovranno essere impartite agli incaricati istruzioni per adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

Deve essere previsto che:

- le credenziali di autenticazione non utilizzate da almeno sei mesi dovranno essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;

- le credenziali dovranno essere disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Devono essere impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Per i casi in cui l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, saranno impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

Sistema di autorizzazione

Nei casi in cui, per gli incaricati, saranno individuati profili di autorizzazione di ambito diverso dovrà essere operativo un sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, dovrà essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Sarà cura del Responsabile del Trattamento assicurarsi, anche per mezzo di personale di sua fiducia e afferente all'Unità operativa, che ad ogni paziente/utente venga fatto firmare il modulo di consenso informato su come saranno trattati i dati di ogni interessato che si avvale dei servizi dell'Azienda, con l'esercizio dell'art. 7 del D. Lgs. 196/03. Il consenso sarà custodito in cartella clinica se trattasi di consenso trattato nei reparti. Il consenso dovrà essere gestito con un'organizzazione di rito, con relativa conservazione, in altre strutture quali: accettazione, ticket, analisi generiche (prelievi, day hospital, ecc.).

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

I dati personali dovranno essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare ogni qualvolta vengano resi disponibili gli aggiornamenti.

Dovranno essere effettuati aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.

Dovranno essere impartite istruzioni organizzative e tecniche per il salvataggio dei dati, con ragionevole frequenza (inizialmente settimanalmente), soprattutto sui singoli PC che non siano collegati ad un Server.

In modo da assicurare la dovuta padronanza di tutti i dipendenti delle Policy del Disaster Recovery e della Business Continuity da regolamentare con l'Amministratore di Sistema aziendale e di concerto col DPO.

Il responsabile del Trattamento dei dati dovrà avviare una elevata collaborazione col DPO Aziendale che dovrà curare la tenuta di un Registro dei Trattamenti, gli adempimenti di data Breach e fungere da interfaccia con la Struttura Garante.

Il calcolo dei Rischi, attuato dal DPO, sarà effettuato in collaborazione con tutti i Responsabili del Trattamento in sinergia con l'art. 32 del regolamento europeo.

Periodicamente il DPO verificherà, con audit interni, il perfetto andamento delle Policy impartite redigendo dei verbali, da sottoporre al Direttore Generale, indicanti l'andamento delle direttive, con cadenza almeno bimestrale, che consentano una piena attuazione del GDPR.

Trimestralmente il DPO convocherà tutti i Responsabili del Trattamento al fine di rendere più performante le attività di trattamento. Ogni Incident di sicurezza dovrà essere reso noto all'intera struttura, per il tramite del DPO, per mezzo di comunicazioni ufficiali mirate alla minimizzazione del rischio.

Dovendo il Responsabile del Trattamento dei dati coordinare l'Organizzazione interna della propria Unità Operativa avrà l'onere di consegnare la Lettera d'incarico al trattamento dei dati personali ad ogni singolo impiegato dell'AOPC facente parte della suddetta Unità Operativa, creando, così, l'Unità Organizzativa di Reparto.

All'uopo si allega un fac-simile di Lettera d'Incarico al trattamento dei dati personali.

Procedura organizzativa:

Occorrerà fare la fotocopia di tale lettera firmata dal Responsabile del Trattamento Direttore dell'Unità Operativa (organizzativa) e consegnarla ad ogni singolo dipendente afferente la struttura di riferimento.

Per comodità si allega anche un foglio contenente ogni singolo dipendente afferente all'Unità (si prega di comunicare tempestivamente al Referente Privacy e/o DPO ogni variazione intervenuta: trasferimenti da e verso la struttura, nuove assunzioni, pensionamenti, altro).

Una volta consegnata la lettera d'incarico al trattamento dei dati personali ad ogni singolo dipendente/incaricato, lo stesso dovrà firmare un elenco di evidenza oggettiva da cui si evinca che la lettera è stata consegnata nella data indicata.

La formazione del personale afferente l'Unità Organizzativa sarà a cura del Responsabile del Trattamento dei dati dell'Unità Operativa; il quale dovrà verificare che tutti i dipendenti che trattano dati presso tale Unità siano stati formati con l'obbligo di indicare al DPO i nominativi di chi ancora non abbia partecipato ai corsi che periodicamente vengono effettuati.

Non sarà ammessa nessuna deroga, in quanto, il trattamento dei dati è sub judice ad una formazione continua e nondimeno, con l'entrata in vigore del GDPR 679/2016, ad esporre l'intera Azienda Ospedaliera a Verifiche da parte del Garante Privacy in funzione anche del Data Breach.

ALLEGATO 5

NOMINA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

Conformemente a quanto stabilito dall'art. 29 del D. Lgs. N. 196/2003 (Codice Privacy) e art. 6 del Regolamento aziendale in materia di Privacy.

Il sottoscritto Direttore generale dell'AOPC- Catanzaro Dott

in qualità di Titolare del trattamento dei dati, presso AOPC- Catanzaro, nomina il Sig.

Rappresentante della Ditta/Società _____ quale Responsabile esterno del Trattamento dei Dati. raccolti nell'ambito del contratto/convenzione per quanto strettamente necessario alla corretta esecuzione del contratto (specificare il contratto);

Elencare i compiti svolti in qualità di Responsabile esterno in relazione al contratto/convenzione stipulato con AOPC - Catanzaro:

- I1 Responsabile esterno del trattamento dei dati dovrà uniformarsi e rispettare il regolamento aziendale sulla privacy, nonché tutta la normativa vigente ed è designato e incaricato dello svolgimento dei seguenti compiti e delle attività:
  - Attenersi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche ispettive periodiche, vigila sulla puntuale osservanza delle proprie istruzioni;
  - Il Responsabile esterno tratterà, per conto e in nome dell'Azienda, i dati personali strettamente necessari all'espletamento del contratto/convenzione;
  - Nominare per iscritto le persone fisiche, incaricate del trattamento;
  - Trasmettere le nomine degli incaricati al titolare di AOPC - Catanzaro;
  - Dare istruzioni ai propri Incaricati per il corretto trattamento dei dati raccolti;
  - Far rispettare agli Incaricati gli obblighi di segretezza e di non divulgazione dei dati;
  - Procedere al trattamento con la dovuta diligenza, attenendosi alle disposizioni contenute nel Codice in materia di protezione dei dati personali, nei relativi provvedimenti di attuazione del Garante, negli atti regolamentari della AOPC - Catanzaro e nella normativa nazionale che disciplina specifici trattamenti di dati;
- Collaborare con il DPO al fine di:
  - Fornirgli le informazioni e gli aggiornamenti necessari, con particolare riferimento ai compiti previsti dal Regolamento aziendale in materia di protezione dei dati personali;
  - Comunicargli qualsiasi mutamento degli elementi del contratto, nonché la cessazione del trattamento di dati;
  - Informarlo tempestivamente di tutte le questioni rilevanti ai fini dell'attuazione del codice e del regolamento aziendale;
  - Non comunicare ad altri soggetti i dati personali di cui venga a conoscenza né

- utilizzarli autonomamente per scopi diversi da quelli sopra menzionati;
- Trattare i dati all'interno della società, soltanto tramite il personale dipendente ed i collaboratori strettamente necessari all'esecuzione delle prestazioni oggetto del contratto, fornendo loro le istruzioni necessarie;
- Trattare i dati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti, e legittimi; i dati devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- Consentire i controlli e la vigilanza sulla corretta osservanza delle disposizioni di legge;
- Trasmettere ad AOPC Catanzaro una descrizione delle misure di sicurezza organizzative e tecniche adottate ad evitare l'accesso non autorizzato, il trattamento non conforme o l'alterazione dei dati personali di proprietà di AOPC- Catanzaro;
- Rispondere alle istanze degli interessati secondo quanto stabilito dal Titolo II del Codice "Diritti dell'interessato" e dal Regolamento aziendale, previo preventivo nulla osta da parte dell'Azienda AOPC- Catanzaro, e predisporre le necessarie modalità organizzative volte a facilitare l'esercizio di accesso dell'interessato;
- Dare riscontro all'interessato che eserciti il diritto di accesso ex art. 7 e seguenti del Codice;
- Dare attuazione ad ogni altro adempimento stabilito dal Titolare del trattamento.

La nomina a Responsabile decadrà in qualunque caso di cessazione del contratto con l'AOPC di Catanzaro, con effetto dalla data di tale cessazione e si intende revocata di diritto alla scadenza del contratto.

Il Responsabile esterno del trattamento dati dichiara di essere a conoscenza di quanto stabilito dal D. Lgs. n. 196/2003 e dal GDPR (UE 2016/679)), nonché dal Regolamento aziendale in materia di Privacy, che viene consegnato in copia,

IL TITOLARE DEL TRATTAMENTO Per accettazione incarico

DIRETTORE GENERALE AOPC IL RESPONSABILE ESTERNO

Dott._____ Dott/Sig.

Catanzaro

Il presente modulo deve essere restituito firmato alla Direzione Generale, entro 30 giorni dalla stipula del contratto/convenzione, che ne darà comunicazione al DPO.

Azienda Ospedaliera Pugliese-Ciaccio: dpo@aocz.it elaborato dalla dott.ssa Sarah Yacoubi
Responsabile Protezione Dati