

# **REGOLAMENTO AZIENDALE PRIVACY E PROTEZIONE DEI DATI PERSONALI**

## ***INDICE:***

### **NORMATIVA E GLOSSARIO**

**ART 1 – L’OGGETTO**

**ART 2 – IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI**

**ART 3 – I DATI PERSONALI TRATTATI DALL’AZIENDA SANITARIA**

**ART 4 – LA POLITICA DI SICUREZZA AZIENDALE**

**ART 5 – LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI**

**ART 6 – IL TRATTAMENTO DI DATI PERSONALI**

**ART 7 – LE RESPONSABILITA’ DEL TRATTAMENTO DEI DATI PERSONALI**

**ART 8 – I RESPONSABILI INTERNI DEL TRATTAMENTO DEI DATI PERSONALI**

**ART 9 – I RESPONSABILI ESTERNI DEL TRATTAMENTO DEI DATI PERSONALI**

**ART 10 – GLI INCARICATI DEL TRATTAMENTO DEI DATI**

**ART 11 – GLI AMMINISTRATORI DI SISTEMA**

**ART 12 – I FACILITATORI PRIVACY DI STRUTTURA**

**ART 13 – IL REFERENTE PRIVACY (DATA PROTECTION OFFICER)**

**ART 14 – L’INFORMATIVA ALL’INTERESSATO**

**ART 15 – IL CONSENSO AL TRATTAMENTO DEI DATI DI SALUTE**

**ART 16 – I DIRITTI DELL’INTERESSATO**

**ART 17 – IL DIRITTO DI ACCESSO E IL DIRITTO ALLA RISERVATEZZA**

**ART 18 – COMUNICAZIONE DI DATI ALL’INTERESSATO**

**ART 19 – IL CENSIMENTO DEL TRATTAMENTO DEI DATI PERSONALI**

**ART 20 – LE MISURE MINIME DI SICUREZZA**

**ART 21 – LE MISURE IDONEE DI SICUREZZA ED IL DOCUMENTO DI ANALISI DEI  
RISCHI**

**ART 22 – LE MISURE MINIME E IDONEE DI SICUREZZA PER I TRATTAMENTI DI  
DATI PERSONALI AFFIDATI A SOGGETTI ESTERNI**

**ART 23 – LA TENUTA IN SICUREZZA DEI DOCUMENTI E ARCHIVI DI TITOLARITA’  
DELL’AZIENDA SANITARIA**

**ART 24 – I LIMITI ALLA CONSERVAZIONE DEI DATI PERSONALI**

**ART 25 – ATTIVITA’ DI VERIFICA E CONTROLLO DEI TRATTAMENTI DI DATI  
PERSONALI**

**ART 26 – IL CONTROLLO A DISTANZA**

**ART 27 – LE NORME TRANSITORIE E FINALI**

**ALLEGATO A) COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO  
DEI DATI PERSONALI**

**ALLEGATO B) ESTRATTO INFORMATIVA**

**ALLEGATO C) ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI  
PERSONALI**

## ***NORMATIVA:***

- D.Lgs. 196/2003 “Codice in materia di protezione dei dati personali”;
- D.Lgs. 82/2005 “Codice Amministrazione digitale”;
- Legge 241/1990 “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi” e ss.mm.ii;
- D.Lgs. 33/2013 “Trasparenza della pubblica amministrazione”;
- Linee guida in tema di Fascicolo sanitario elettronico (FSE) e Dossier sanitario- 16 Luglio 2009;
- 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 - 28 Maggio 2014;
- Linee guida in materia di Dossier sanitario - 4 Giugno 2015.

## ***GLOSSARIO:***

Trattamento di dati personali: qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

Titolare: persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile: persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali. Individuati tra coloro che per esperienza, capacità ed affidabilità sono in grado di fornire idonea garanzia del pieno rispetto delle indicazioni del presente Regolamento e della normativa vigente.

Incaricati: persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile.

Interessato: persona fisica cui si riferiscono i dati personali.

Dato personale: qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato.

Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. I dati di salute non possono essere diffusi. I dati sensibili sono oggetto di comunicazione anche verso soggetti pubblici solo se prevista da disposizioni di legge o di regolamento.

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Comunicazione: il dare conoscenza dei dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

## **Art. 1 - L' OGGETTO**

Lo scopo primario del presente Regolamento è quello di assicurare che il trattamento dei dati di pertinenza dell'Azienda Sanitaria Toscana Nord Ovest (di seguito Azienda Sanitaria), nella sua qualità di Titolare del trattamento dei dati personali, avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con la medesima, secondo le disposizioni vigenti in materia di protezione dei dati e amministrazione digitale.

L'Azienda Sanitaria garantisce il rispetto dei principi di necessità, pertinenza e non eccedenza nel trattamento dei dati personali e adotta al suo interno tutte le misure correttive per la loro applicazione.

L'Azienda Sanitaria assicura l'adozione di misure di sicurezza, anche preventive, idonee ad evitare situazioni di rischio e di non conformità o di alterazione dei dati tese ad assicurare l'integrità del patrimonio informativo aziendale.

L'Azienda adotta tutte le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato come previsto dalle disposizioni vigenti.

## **Art. 2 - IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI**

Il Titolare del trattamento dei dati personali è l'Azienda Sanitaria.

Il Titolare, tramite il Referente Privacy (DPO) di cui all'art.12 del presente regolamento, provvede, nei casi previsti dalla legge:

- a) ad assolvere l'obbligo di notificazione all'Autorità Garante;
- b) a richiedere a tale Autorità l'autorizzazione al trattamento dei dati sensibili, ove necessaria;
- c) ad adottare, per quanto di competenza, le misure necessarie a garantire la protezione dei dati personali, anche per quanto riguarda il processo di digitalizzazione;
- d) a nominare i Responsabili Interni ed Esterni del trattamento di dati personali impartendo loro le necessarie istruzioni per la corretta gestione e protezione dei dati personali;

Il Titolare del trattamento è tenuto, in base alle disposizioni vigenti in materia di protezione dei dati, ad effettuare nei confronti di tutti i Responsabili del trattamento le verifiche e controlli sulla correttezza del trattamento dei dati loro assegnato.

## **Art. 3 - I DATI PERSONALI TRATTATI DALL'AZIENDA SANITARIA**

L'Azienda Sanitaria, tratta le informazioni relative a:

- Cittadini utenti, assistiti e loro familiari e/o accompagnatori
- Personale in rapporto di dipendenza, convenzione o collaborazione
- Soggetti che per motivi di studio o volontariato frequentano le strutture dell'Azienda Sanitaria
- Clienti e fornitori

## **Art. 4 - LA POLITICA DI SICUREZZA AZIENDALE**

L'Azienda Sanitaria, anche in considerazione dell'estrema delicatezza dei dati oggetto di trattamento, della loro numerosità e della numerosità dei soggetti che necessariamente devono trattare dati personali, assicura che il trattamento dei dati personali avvenga con modalità tali da preservarne l'integrità e la confidenzialità, nel rispetto delle misure minime e delle misure idonee di sicurezza.

Al riguardo attiva le necessarie risorse organizzative, tecnologiche e finanziarie perché il trattamento dei dati personali sia conforme alle disposizioni in materia di protezione dei dati e di amministrazione digitale.

## **Art. 5 - LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI**

Il Titolare prima di procedere al trattamento dei dati effettua una valutazione preliminare dell'impatto delle operazioni di trattamento, avvalendosi del Referente Privacy (D.P.O.)

La valutazione di impatto preliminare è effettuata nei casi e nei modi previsti dalle disposizioni vigenti, al fine di valutare i rischi del trattamento, le misure previste per contenerli, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità alle norme vigenti, tenuto conto dei diritti degli interessati e delle finalità del trattamento.

L'Azienda Sanitaria, inoltre, attiva tutte le azioni necessarie al rispetto delle misure e prescrizioni specifiche individuate dall'Autorità Garante Privacy per il corretto trattamento dei dati, in modo particolare per quanto riguarda i trattamenti resi possibili dai processi di innovazione digitale e dai diversi modelli di sistemi informativi sanitari integrati.

#### **Art. 6 - IL TRATTAMENTO DI DATI PERSONALI**

Il trattamento dei dati personali è ammesso solo da parte del Titolare del trattamento dei dati, dei Responsabili Interni ed Esterni del trattamento dei dati, degli Incaricati e degli Amministratori di Sistema.

All'interno dell'Azienda sono individuati i ruoli e i compiti dei soggetti autorizzati a trattare i dati di pertinenza del Titolare del trattamento dei dati personali

È illecito il trattamento di dati personali da parte di soggetti non formalmente autorizzati dall'Azienda Sanitaria a trattare i dati.

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'Interessato.

Oggetto del trattamento devono essere i soli dati essenziali per svolgere attività istituzionali.

I dati personali devono essere trattati in modo lecito, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini non incompatibili con tali scopi.

I Responsabili sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'Interessato fornisce di propria iniziativa.

I Responsabili, gli Incaricati e gli Amministratori di Sistema sono autorizzati all'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento dei dati personali è consentito.

I Responsabili sono tenuti a comunicare dati personali e/o sensibili agli altri Responsabili del trattamento solo in caso di necessità, ovvero quando non sia possibile perseguire le stesse finalità con dati anonimi o aggregati.

In particolare, i Responsabili del trattamento Interni ed Esterni relativi alla gestione, protezione e manutenzione dei sistemi informativi e dei programmi informatici dovranno assicurare al Titolare che tali sistemi e programmi siano configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

I dati che, anche a seguito di verifica, risultino eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.

I trattamenti di dati effettuati utilizzando le banche dati di più Titolari, sono autorizzati nelle sole ipotesi previste da espressa disposizione di legge o previa specifica autorizzazione da parte dell'Autorità Garante.

#### **Art. 7 - LE RESPONSABILITA' DEL TRATTAMENTO DEI DATI PERSONALI**

Il Titolare designa i Responsabili del trattamento dei dati personali cui delegare il coordinamento delle attività di trattamento dei dati personali.

I Responsabili del trattamento si distinguono in Responsabili Interni e Responsabili Esterni del trattamento dei dati personali. I Responsabili interni sono nominati dal Titolare con la Deliberazione che conferisce loro l'incarico a Responsabile di struttura, preventivamente allo svolgimento delle attività di trattamento dei dati.

La nomina dei Responsabili del trattamento dei dati, accompagnata dalle specifiche indicazioni operative per il corretto assolvimento dei compiti a questi delegati in materia di protezione dei dati, dovrà essere notificata per iscritto ai soggetti individuati a cura del Referente Privacy (DPO).

La funzione di Responsabile del trattamento dei dati è attribuita personalmente e non è suscettibile di delega.

L'elenco dei Responsabili del trattamento dei dati in ambito aziendale è tenuto a cura del Referente Privacy (D.P.O.).

I Responsabili del trattamento dei dati personali compiono tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di riservatezza, sicurezza e protezione dei dati personali relativamente ai trattamenti loro assegnati; in particolare hanno il dovere di osservare e fare osservare:

- le misure di sicurezza e le altre precauzioni individuate nel Documento di Analisi dei Rischi adottato dall'Azienda;

- le disposizioni relative alle misure di sicurezza emanate dall'Azienda Sanitaria, le ulteriori linee guida sulla riservatezza dei dati, la protezione delle informazioni e sull'amministrazione digitale.

I Responsabili del trattamento dei dati sono dotati di autonomia gestionale ed organizzativa per il trattamento dei dati di propria competenza; questi sono tenuti, inoltre, ad adottare ogni misura necessaria per il rispetto della riservatezza nell'erogazione delle prestazioni e dei servizi sanitari.

E' compito dei Responsabili del trattamento dei dati verificare che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza rispondano ai principi di necessità, pertinenza e non eccedenza, segnalando al Titolare ed al Referente Privacy (D.P.O.) eventuali situazioni di potenziale compromissione della protezione dei dati personali.

I Responsabili del trattamento, relativamente al proprio settore di competenza, rispondono al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di riservatezza, sicurezza, protezione dei dati e amministrazione digitale e riferiscono periodicamente a questi e al Referente Privacy (D.P.O.) su come svolgono i compiti specifici loro assegnati.

I Responsabili del trattamento dei dati nominano formalmente gli Incaricati del trattamento, fornendo loro per iscritto istruzioni operative dettagliate e specifiche sulle corrette modalità di trattamento dei dati personali e vigilano sul rispetto di tali istruzioni.

#### **Art. 8 - I RESPONSABILI INTERNI DEL TRATTAMENTO DEI DATI PERSONALI**

Ai sensi dell'art. 29 del D.Lgs. n. 196/03 sono nominati, con il provvedimento di conferimento, quali Responsabili interni del trattamento dei dati personali, i dipendenti che ricoprono gli incarichi di Direttore o Responsabile di: Direzione di U.O., Struttura funzionale, Dipartimento, Area, Presidio Ospedaliero, Staff, Zona Distretto.

Sono altresì nominati Responsabili interni del trattamento i dipendenti che svolgono attività libero-professionale intra-moenia e i Responsabili degli studi clinici. La nomina è effettuata con il provvedimento di autorizzazione allo svolgimento di tali attività, con atto predisposto a cura degli uffici competenti.

L'Azienda, tramite IL Referente Privacy, provvede annualmente alla ricognizione degli incarichi di cui sopra, il cui elenco, costantemente aggiornato, è pubblicato sul sito aziendale.

I Responsabili del trattamento si attengono agli obblighi di cui al Codice Privacy e al presente Regolamento, e più specificamente ai compiti e alle istruzioni allegati al presente Regolamento sotto la lettera A), consultabili sul sito aziendale, notificati unitamente alla comunicazione della nomina a cura del Referente Privacy.

Le Strutture Aziendali deputate alla gestione delle risorse umane sono tenute a trasmettere tempestivamente al Referente Privacy (D.P.O.) ogni conferimento o modifica di responsabilità in ambito aziendale.

#### **Art. 9 - I RESPONSABILI ESTERNI DEL TRATTAMENTO DEI DATI PERSONALI**

Ai sensi dell'art. 29 del Codice, la qualità di Responsabile Esterno del trattamento dei dati, è attribuita ai soggetti esterni all'Azienda cui vengono delegate attività di competenza aziendale o che svolgono attività connesse, strumentali e di supporto, ivi incluse le attività manutentive, che comportano l'uso di dati personali, comuni e/o sensibili.

In tutti gli atti che disciplinano rapporti con i soggetti di cui al precedente comma (contratti, convenzioni, scritture private, conferimenti, etc.), devono essere inserite al fine di assicurare il corretto trattamento dei dati personali, specifiche "clausole di garanzia" con le quali il soggetto terzo si impegna

all'osservanza delle norme sulla protezione dei dati personali e sulla tutela del sistema informativo aziendale, nonché a quanto disposto dall'Azienda al riguardo.

L'Azienda provvede, a seguito della sottoscrizione del contratto, a nominare formalmente tali soggetti quali responsabili esterni.

All'Ufficio Privacy deve pervenire da parte dei Responsabili dei procedimenti (aziendali, di Estar e di altri soggetti terzi) comunicazione della clausola di garanzia. La clausola di garanzia rappresenta l'atto di nomina in sé e per sé, mentre l'atto di nomina "ad hoc" si considera ipotesi residuale, necessario quando nel procedimento di individuazione del soggetto esterno non è stato possibile conferire tale responsabilità con provvedimento a firma del Direttore Generale, Titolare del trattamento.

#### **Art. 10 - GLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI**

Gli Incaricati del trattamento dei dati personali sono le persone fisiche che effettuano le operazioni di trattamento di dati personali e/o sensibili nominati a tale scopo dal Responsabile del trattamento.

Sono a tale scopo da designare come Incaricati sia i dipendenti dell'Azienda che i collaboratori che, a qualsiasi titolo (ad esempio: tirocinanti, studenti, stagisti, volontari, liberi professionisti, borsisti), prestino la loro opera all'interno delle strutture dell'Azienda.

Per la loro designazione è utilizzata apposita modulistica, che prevede la trascrizione della data di inizio e fine attività all'interno della struttura.

Gli Incaricati ricevono formale atto di designazione dai loro Responsabili del trattamento, che impartiscono loro disposizioni sul corretto uso dei dati, in special modo sotto il profilo della sicurezza e vengono informati sulle direttive vigenti sulla protezione dei dati da loro trattati.

L'atto di designazione ad Incaricato costituisce l'unico presupposto di liceità per l'uso dei dati personali e/o sensibili in ambito aziendale; tale atto, controfirmato per presa visione dall'Incaricato, è conservato a cura del Responsabile.

#### **Art. 11 - GLI AMMINISTRATORI DI SISTEMA**

Il Titolare del trattamento dei dati affida ai Responsabili Esterni del trattamento dei dati cui sono state delegate competenze di gestione e protezione dei sistemi informativi e delle risorse hardware e software dell'Azienda Sanitaria, l'onere di coordinare l'attività degli Amministratori di Sistema e presidiare tutti gli adempimenti in materia previsti dalla normativa vigente, compreso la loro designazione ed il rispetto delle misure di controllo dell'attività.

Al riguardo tali Responsabili sono pertanto tenuti ad assolvere a tutte le misure previste dai Provvedimenti dell'Autorità Garante in tema di Amministratore di Sistema ed a trasmettere al Titolare del trattamento sia l'evidenza delle nomine e delle ulteriori misure adottate che la copia della relativa documentazione entro il mese di gennaio di ogni anno solare.

Tali Responsabili del trattamento sono tenuti a depositare presso la struttura del Data Protection Officer dell'Azienda Sanitaria, la copia degli atti con cui sono stati designati gli amministratori di sistema.

#### **Art. 12 - I FACILITATORI PRIVACY DI STRUTTURA**

L'Azienda Sanitaria si avvale di una rete di collaboratori, denominati Facilitatori Privacy di struttura, che, all'interno di ogni struttura aziendale, supportano le azioni tese al rispetto delle normative sulla riservatezza, trasparenza e amministrazione digitale.

Tale funzione è di norma assicurata dai R.A.Q. (Responsabile Qualità e Accreditamento) o in via alternativa da personale adeguatamente formato.

Questi collaborano con il Responsabile del trattamento e con Referente Privacy (D.P.O.) per l'eliminazione ed il contenimento delle criticità relative alla gestione e protezione dell'informazione.

Il Facilitatore Privacy di struttura è individuato e nominato dal Responsabile del trattamento dei dati e comunicazione di tale nomina viene trasmessa al Referente Privacy (D.P.O.).

Il Facilitatore Privacy riceve dal Titolare una formazione continua e specifica sulla normativa che regola il trattamento dei dati personali e sensibili e su ogni altra disposizione relativa alla gestione e protezione dell'informazione.

### **Art. 13 - IL REFERENTE PRIVACY (DATA PROTECTION OFFICER)**

La Struttura del Referente Privacy ha funzione di riferimento in materia di protezione dei dati personali e coordina l'applicazione delle disposizioni di legge che riguardano la gestione e protezione dell'informazione, adeguandola agli specifici percorsi organizzativi dell'Azienda, anche per garantire il rispetto delle misure di sicurezza.

La struttura del Referente Privacy, svolge i seguenti compiti:

1. assiste la Direzione Aziendale nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati per quanto riguarda gli adempimenti derivanti dalla normativa sulla riservatezza dei dati;
2. cura la gestione delle nomine a Responsabile del trattamento;
3. provvede alla stesura del Documento di Analisi dei Rischi (DAR) avvalendosi della necessaria collaborazione dei Responsabili interni ed esterni del trattamento dei dati e degli Amministratori di Sistemi;
4. vigila sull'osservanza del presente Regolamento Aziendale, fornendo la necessaria consulenza in ordine alle problematiche in tema di riservatezza, protezione dei dati;
5. svolge l'attività di formazione aziendale in tema di normativa sulla riservatezza, protezione dei dati;
6. fornisce risposta ai quesiti che vengono sottoposti alla sua attenzione da parte delle strutture aziendali relativamente al trattamento dei dati personali;
7. gestisce le istanze degli Interessati per quanto riguarda il trattamento e la protezione dei loro dati personali;
8. partecipa all'adeguamento dei percorsi aziendali per quanto attiene l'aspetto della riservatezza, della protezione dei dati e del rispetto della dignità dell'ammalato, che siano condivisibili su tutto il territorio aziendale;
9. provvede, su iniziativa dei Responsabili del trattamento dei dati, alla revisione ed integrazione della modulistica in uso in ambito aziendale per quanto concerne il profilo della riservatezza nell'uso dei dati;
10. integra, anche su iniziativa dei Responsabili del trattamento, i capitoli, i contratti e le convenzioni e accordi di servizio che vengono stipulati dall'Azienda o per conto della stessa, e che prevedono un trattamento di dati personali delle opportune indicazioni sulla loro protezione;
11. partecipa a richiesta agli audit che coinvolgono gli aspetti relativi alla normativa in materia di protezione dei dati;
12. fornisce pareri nel rispetto dei requisiti in materia di privacy per la predisposizione dei capitoli di gara dei sistemi informatici e apparecchiature elettromedicali;
13. provvede, previa comunicazione dei Responsabili del trattamento dei dati, a segnalare all'Autorità Garante Privacy e agli Interessati i casi di anomalie e/o violazione dei dati personali (data breach);
14. costituisce punto di contatto dedicato per l'Autorità Garante per tutto quanto concerne il trattamento dei dati;
15. cura che la comunicazione di dati personali da parte dell'Azienda avvenga nel rispetto delle norme di Legge o di Regolamento, inoltrando se necessario specifica istanza all'Autorità Garante per la Privacy.

La comunicazione da parte dell'Azienda Sanitaria di dati personali a soggetti privati è ammessa solo quando prevista da una norma di legge o di regolamento.

I dati sensibili sono oggetto di comunicazione, anche verso soggetti pubblici, solo se previsto da disposizione di Legge o di Regolamento.

I dati di salute e giudiziari non possono in alcun caso essere oggetto di diffusione.

### **Art. 14 - L' INFORMATIVA ALL'INTERESSATO**

L'azienda adotta un modello di informativa chiaro e comprensibile all'utenza, sulla base dell'estratto allegato B) al presente regolamento, contenente le informazioni previste dalla normativa vigente relativamente a :

- finalità e modo d'uso dei dati;
- obbligatorietà o meno del conferimento dei dati;
- conseguenze di un eventuale rifiuto a fornire i dati;
- coloro ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;

- come possono essere esercitati i diritti di accesso in base alle disposizioni vigenti;
- il nome e la sede di lavoro del Responsabile e degli Incaricati.

L'Azienda Sanitaria predispone ulteriori informative specifiche avvalendosi del Referente Privacy (D.P.O.) che rappresentano gli ulteriori e particolari trattamenti di dati svolti sotto il coordinamento di ogni singolo Responsabile del trattamento.

L'informativa all'Interessato viene resa anche per estratto tramite l'affissione di appositi manifesti o la somministrazione di appositi documenti nei locali di accesso all'utenza, secondo procedure e modelli concordati con il Referente Privacy (D.P.O.).

L'Azienda attiva, utilizzando i sistemi Internet ed Intranet, adeguate modalità di visibilità delle azioni poste in essere all'interno dell'Azienda in attuazione della normativa sulla riservatezza dei dati e degli ulteriori indirizzi regionali in materia.

## **Art. 15 - IL CONSENSO AL TRATTAMENTO DEI DATI DI SALUTE**

L'Azienda tratta i dati idonei a rivelare lo stato di salute a fini di cura, dopo avere erogato specifica informativa:

- a) previa acquisizione del consenso dell'Interessato se il trattamento riguarda dati ed operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'Interessato;
- b) senza il consenso dell'Interessato, ma previa autorizzazione dell'Autorità Garante per la Privacy, se la finalità di cui alla lettera precedente riguarda un terzo o la collettività.
- c) senza il consenso dell'interessato, se i dati sono trattati per finalità non di cura.

L'Azienda acquisisce il consenso al trattamento dei dati anche a mezzo annotazione sia cartacea che nelle procedure informatiche.

L'Azienda acquisisce uno specifico consenso in occasione di trattamenti particolarmente complessi.

Il Titolare assicura attraverso idonee modalità l'archiviazione dei consensi espressi dagli interessati in modo da rendere fruibili e rintracciabili le autorizzazioni da questi rilasciate.

## **Art. 16 - I DIRITTI DELL'INTERESSATO**

L'Interessato ha diritto di:

1. avere informazioni sull'esistenza o meno di propri dati personali che siano in possesso dell'Azienda, indicazione della loro origine, delle finalità e modalità del trattamento;
2. chiedere la modifica, il blocco del trattamento o la cancellazione dei propri dati, se i dati non sono gestiti o custoditi per obbligo di legge;
3. conoscere i Responsabili e/o Incaricati che trattano le sue informazioni e i soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza;
4. visionare gli accessi ai propri dati;
5. essere informato dei data breach che coinvolgono dati personali di proprio riferimento;
6. esercitare il diritto di oscuramento e deoscuramento previsto dalla normativa vigente;
7. integrare, rettificare, aggiornare i dati trattati di proprio riferimento, mediante annotazione delle modifiche richieste senza alterare la documentazione di riferimento.

L'Interessato può avanzare specifica istanza, come da modello Allegato C) al presente Regolamento, al Titolare del trattamento, anche attraverso l'Ufficio Relazioni per il Pubblico, che la trasmette per competenza al Referente Privacy (D.P.O.).

Il Referente Privacy (D.P.O.) avvia il procedimento, avvalendosi necessariamente dell'apporto e della collaborazione del Responsabile del trattamento dei dati di competenza e degli Amministratori di Sistema interessati.

L'Interessato ha diritto ad ottenere risposta entro 15 giorni dalla data di ricevimento dell'istanza; tale termine è prorogato in caso di necessità di ulteriori indagini o verifiche da parte del Referente Privacy (D.P.O.). Di ciò sarà data comunicazione all'Interessato entro e non oltre 3 giorni dal ricevimento dell'istanza stessa.

L'Interessato avrà diritto comunque ad ottenere una risposta entro 60 giorni, decorrenti dalla data di ricevimento dell'istanza.



L'Interessato, nell'esercizio dei diritti sopra riportati può conferire per iscritto, delega o procura a persone fisiche o ad associazioni; se tali diritti sono riferiti a dati personali concernenti persone decedute possono essere esercitati da chiunque vi abbia un interesse giuridicamente rilevante.

#### **Art. 17 - IL DIRITTO DI ACCESSO E IL DIRITTO ALLA RISERVATEZZA**

L'Azienda Sanitaria, in osservanza delle disposizioni vigenti in tema di riservatezza e di trasparenza, valuta anche con riguardo ad altre regolamentazioni specifiche, caso per caso la possibilità degli interessati di accedere ai documenti.

L'accesso ai dati idonei a rivelare lo stato di salute o le abitudini sessuali è ammesso solo quando il diritto da tutelare, tramite istanza di accesso, è di rango di almeno pari al diritto alla riservatezza, ovvero consiste in un diritto alla personalità o in un altro diritto o libertà fondamentale o inviolabile, quale ad esempio il diritto alla difesa.

Ulteriori specifiche indicazioni agli operatori sono contenute nelle istruzioni operative adottate dall'Azienda.

#### **Art. 18 – COMUNICAZIONE DI DATI ALL'INTERESSATO**

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo attraverso:

- a) la consegna dei dati al medico di fiducia che, a sua volta, li renderà noti all'Interessato;
- b) una spiegazione orale o un giudizio scritto da parte di un medico del servizio interessato o, su specifica delega scritta, da parte di operatore sanitario;
- c) modalità telematiche nei casi e nei modi previsti dalla specifica normativa.

La documentazione sanitaria che viene consegnata in busta chiusa può essere ritirata dall'Interessato o da altra persona diversa da questo delegata, salvo il caso dei documenti relativi a dati regolati da normative speciali che prevedono il ritiro diretto dell'interessato.

#### **Art. 19 - IL CENSIMENTO DEL TRATTAMENTO DEI DATI PERSONALI**

L'Azienda Sanitaria individua come elementi fondamentali delle politiche di protezione dei dati personali:

- l'analisi dei trattamenti di dati personali
- la distribuzione dei compiti e delle responsabilità attribuite a coloro che trattano dati personali.

L'Azienda Sanitaria, attraverso il CE.TRA (Censimento Trattamento Dati Personali), provvede alla rilevazione dei trattamenti suddivisi per tipologia e per struttura organizzativa e ogni altro elemento necessario ad individuare le responsabilità relative al trattamento dei dati personali.

Il CE.TRA, sulla base delle rilevazioni di cui in precedenza individua:

- i diversi livelli di responsabilità attribuiti in relazione al trattamento dei dati, suddivisi per Responsabili del trattamento ed Amministratori di Sistema;
- i trattamenti che vengono svolti e per ognuno di questi i soggetti autorizzati (Incaricati) a gestire le basi di dati sia cartacee che automatizzate.

Il CE.TRA è costantemente aggiornato a cura del Referente Privacy (D.P.O.).

#### **Art. 20 - LE MISURE MINIME DI SICUREZZA**

Il Titolare e i Responsabili del trattamento dei dati sono tenuti ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati e amministrazione digitale, ogni misura di sicurezza necessaria per assicurare un livello sufficiente di sicurezza dei dati personali trattati dall'Azienda Sanitaria.

Ogni Responsabile Interno del trattamento, avvalendosi anche del Facilitatore Privacy di struttura, è tenuto a verificare che i propri collaboratori adottino tutte le misure necessarie alla protezione dei dati.

L'accesso alle procedure informatiche è consentito solo utilizzando apposite credenziali di autorizzazione composte da un user-id, attribuito dall'Amministratore di Sistema di competenza, e da una password.

Il rilascio dell' user-id all'incaricato avviene previa formale richiesta a firma congiunta dell'Incaricato e del Responsabile del Trattamento dei Dati, che verifica la congruenza di tale richiesta con l'atto di nomina ad Incaricato.

La richiesta, una volta sottoscritta dal Responsabile del trattamento, è inoltrata all'Amministratore di Sistema di competenza che, una volta attribuite le relative credenziali, la inoltra al Referente Privacy (D.P.O.), presso la cui struttura sono depositati gli originali degli atti di nomina ad incaricato.

La struttura Referente Privacy (D.P.O.) verifica la congruenza della nomina ad incaricato con la richiesta del Responsabile di rilascio delle credenziali e segnala a questi ogni eventuale anomalia.

L'Incaricato modifica la password rilasciata dall'Amministratore di sistema in occasione del primo accesso, individuandone una segreta che soddisfi i requisiti di sicurezza previsti dalla normativa vigente.

La password è strettamente personale e a nessun titolo può essere comunicata a terzi; della sua riservatezza risponde personalmente il singolo Incaricato del trattamento dei dati personali .

Il Responsabile del trattamento dei dati è tenuto a comunicare agli Amministratori di Sistema e al Referente Privacy (D.P.O.) la data di cessazione dell'incarico al trattamento dei dati da parte del suo collaboratore; della mancata comunicazione risponde, per omessa adozione di misure minime di sicurezza, il Responsabile del trattamento.

Spetta all'U.O. Amministrazione del Personale comunicare all'Amministratore di Sistema gli aggiornamenti e le variazioni relative al personale (cessazioni, sostituzioni, incarichi, aspettative, assenze prolungate per almeno 180 gg, trasferimenti, ecc.)

## **Art. 21 - LE MISURE IDONEE DI SICUREZZA E IL DOCUMENTO DI ANALISI DEI RISCHI**

L'Azienda individua le risorse strumentali, umane e finanziarie necessarie per attivare le misure idonee di sicurezza previste dalle disposizioni vigenti in tema di protezione dei dati ed amministrazione digitale. L'Azienda adotta, entro il 30 Giugno di ogni anno, un Piano Analisi Rischi Privacy (di seguito P.A.R.P.), che:

- individua le misure idonee per elevare lo standard di sicurezza dei dati anche sulla base dell'analisi dei rischi;
- rappresenta la distribuzione dei compiti e delle responsabilità del trattamento dei dati;
- programma l'attività di formazione degli Incaricati, dei Responsabili del trattamento e Amministratori di Sistema al fine di un utilizzo consapevole delle informazioni;
- evidenzia le misure che l'Azienda Sanitaria ha adottato nel tempo per proteggere i dati personali a sua disposizione e il piano delle azioni di miglioramento che intende adottare per l'anno in corso.

Il P.A.R.P. è predisposto dal Referente Privacy (D.P.O.) sulla base delle informazioni trasmesse dai Responsabili Interni ed Esterni del trattamento dei dati, degli amministratori di sistema e della rete dei Facilitatori privacy.

Nella relazione annuale, che i Responsabili del trattamento dei dati devono inviare al Referente Privacy (D.P.O.) entro il 31 gennaio di ogni anno, deve essere evidenziato:

- l'attività svolta e le misure di sicurezza adottate;
- le carenze strutturali e organizzative;
- le specifiche necessità formative necessarie per l'attuazione delle disposizioni sulla riservatezza;
- le criticità di sicurezza riscontrate;
- le contromisure di cui si propone l'attivazione.

## **Art. 22 - LE MISURE MINIME E IDONEE DI SICUREZZA PER I TRATTAMENTI DI DATI PERSONALI AFFIDATI A SOGGETTI ESTERNI**

I Responsabili esterni del trattamento sono tenuti ad assicurare al Titolare del trattamento di aver adottato, prima di effettuare attività di trattamento di dati, ogni misura minima di sicurezza prevista dalla normativa vigente in tema di protezione di dati e amministrazione digitale.

Tali soggetti sono comunque tenuti ad assicurare al Titolare del trattamento il rispetto delle specifiche istruzioni operative impartite dall'Azienda Sanitaria per la tenuta in sicurezza dei dati oggetto di

affidamento e di aver ulteriormente attivato ogni altra misura idonea alla protezione dei dati di titolarità dell'Azienda Sanitaria.

Tali responsabili sono tenuti ad inviare al Referente Privacy (D.P.O.) entro il 31 gennaio di ogni anno, una relazione dettagliata nella quale sono evidenziate:

- l'elenco delle risorse hardware e software disponibili,
- le procedure di continuità operativa ed emergenza adottate,
- le misure di recupero da disastro adottate,
- le misure di back-up del sistema informativo aziendale e di contenimento dei virus informatici, comprese quelle di conservazione sostitutiva,
- le eventuali criticità che potrebbero costituire occasione di accesso non consentito o perdita/manomissione del patrimonio informativo gestito dall'azienda,
- le misure adottate per la cifratura, o la separazione dei dati relativi alla salute,
- le misure adottate per la gestione delle disposizioni in tema di Amministratori di Sistema, rimettendo al riguardo anche la relativa documentazione.

Nel caso in cui il Responsabile Esterno del trattamento nell'esecuzione delle attività di trattamento utilizzi strumenti informatici propri, è tenuto a certificare con propria dichiarazione scritta di assicurare la protezione dei dati affidati dal Titolare attraverso specifiche misure minime di sicurezza e non aver affidato alcune fasi del trattamento a soggetti terzi.

Qualora il Responsabile Esterno del trattamento utilizzi, al contrario, strumenti informatici forniti dall'Azienda Sanitaria, è tenuto a trasmettere copia degli atti di designazione a Incaricati al Referente Privacy (D.P.O.) che provvederà ad attivare le procedure necessarie al rilascio delle relative credenziali di accesso.

Il mancato rispetto da parte del Responsabile del trattamento delle misure minime e idonee di sicurezza può costituire titolo per la rescissione del rapporto sottostante l'attivamento del trattamento dei dati ed ogni altra azione per eventuale risarcimento del danno.

## **Art. 23 - LA TENUTA IN SICUREZZA DEI DOCUMENTI E ARCHIVI DI TITOLARITA' DELL'AZIENDA SANITARIA**

Gli archivi che custodiscono i dati di cui è titolare del trattamento l'Azienda sanitaria, cartacei e digitali, devono essere collocati in locali non esposti a rischi ambientali in ossequio alle disposizioni generali in materia di sicurezza e a quelle specifiche per la protezione del patrimonio informativo aziendale in tema di Continuità Operativa, Conservazione Sostitutiva e Disaster Recovery.

L'accesso agli archivi cartacei aziendali è formalmente autorizzato, da parte dei Responsabili Interni ed Esterni del trattamento; il rilascio di tale autorizzazione, relativamente agli archivi digitali, è di competenza dell'Amministratore di Sistema previa indicazione del Responsabile del Trattamento.

Gli archivi cartacei e digitali sono oggetto di trattamento da parte del Responsabile del trattamento dei dati di competenza, che deve assicurarne la riservatezza, protezione ed integrità per tutto il tempo in cui ne mantiene la disponibilità.

Per quanto riguarda la documentazione cartacea facente parte dell'archivio aziendale storico e/o di deposito, in conformità a quanto disposto dal Ministero per i beni Culturali ed Ambientali con l'apposito Massimario di scarto per gli archivi degli Enti Sanitari, periodicamente l'Azienda predispone un piano di scarto d'archivio, approvato con apposita deliberazione.

L'Azienda, relativamente agli archivi informatizzati di dati, adotta, facendo seguito alle disposizioni vigenti in tema di protezione dati e amministrazione digitale, avvalendosi del Referente Privacy (D.P.O.) e dei suoi Responsabili Interni ed Esterni del trattamento dei dati e degli Amministratori di Sistema, idonee procedure di:

- salvataggio periodico degli archivi di dati personali;
- misure di contenimento dei virus informatici;
- disaster recovery;
- continuità operativa;
- conservazione sostitutiva.

#### **Art. 24 - I LIMITI ALLA CONSERVAZIONE DEI DATI PERSONALI**

L'Azienda assicura l'adozione di procedure attraverso le quali:

- si proceda alla distruzione dei documenti analogici e digitali, una volta terminato il limite minimo di conservazione dei documenti e dei dati in questi riportati;
- lo smaltimento di apparati hardware o supporti rimovibili di memoria non renda possibile accedere ad alcun dato personale di cui è titolare l'Azienda Sanitaria;
- il riutilizzo di apparati di memoria o hardware non renda possibile accedere ad alcun dato personale di cui è titolare l'Azienda Sanitaria.

#### **Art. 25 - ATTIVITA' DI VERIFICA E CONTROLLO DEI TRATTAMENTI DI DATI PERSONALI**

L'Azienda individua con apposito atto le modalità attraverso cui si svolgono le attività di verifica e controllo del rispetto delle misure di legge e delle ulteriori disposizioni impartite durante le operazioni di trattamento dei dati da parte dei responsabili Interni, Esterni, Amministratori di Sistema e Incaricati del trattamento.

I controlli e le verifiche sono effettuati previa programmazione periodica o in caso di necessità anche su sollecitazione degli interessati e le relative attività sono svolte dal Nucleo Controlli Trasversali al quale il Referente Privacy (D.P.O.) partecipa quale componente, la cui attività è disciplinata da apposite procedure.

#### **Art. 26 - IL CONTROLLO A DISTANZA**

Ad ogni sistema di controllo a distanza, degli Interessati e/o del lavoratore, l'Azienda Sanitaria applica il principio di proporzionalità tra mezzi impiegati e fini perseguiti, nel rispetto delle disposizioni vigenti e delle ulteriori direttive dell'Autorità Garante per la protezione dei dati personali.

L'Azienda comunque garantisce il rispetto della disciplina del divieto di controllo a distanza del lavoratore, così come prevista dalla normativa di riferimento compreso il rispetto degli accordi con le rappresentanze sindacali aziendali, adottando i conseguenti regolamenti applicativi.

Per tutti i sistemi di controllo attivati dall'Azienda Sanitaria, questa deve assicurare l'effettività delle misure di tutela degli interessati e dei lavoratori, in particolare per quanto riguarda l'erogazione di specifica informativa e la piena trasparenza delle caratteristiche, finalità e modalità del controllo operato.

#### **Art. 27 - LE NORME TRANSITORIE E FINALI**

Per tutto quanto non espressamente previsto dal presente Regolamento si applica la normativa vigente in tema di protezione dei dati personali e amministrazione digitale.

L'Azienda Sanitaria si riserva, inoltre, di adeguare e modificare il testo del presente Regolamento qualora la normativa e le direttive sopra citate lo rendano opportuno.

**Compiti ed istruzioni per i Responsabili  
del trattamento dei dati personali**

ai sensi del 'Codice in materia di protezione dei dati personali' (D.Lgs. 196/2003)

**PRINCIPI GENERALI DA OSSERVARE**

Il Responsabile del trattamento dei dati personali, di seguito per brevità chiamato Responsabile, deve trattare i dati:

- secondo il principio di liceità, vale a dire conformemente alle disposizioni di legge e regolamentari, ed in particolare del D. Lgs. 196/03, di seguito chiamato Codice Privacy
- secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui
- in osservanza delle norme di cui al Codice di Comportamento dei dipendenti dell'Azienda e delle altre disposizioni applicabili in materia.

I dati devono essere raccolti solo per scopi:

- ✓ determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
- ✓ espliciti, nel senso che il soggetto interessato ha diritto ad essere informato sulle finalità del trattamento;
- ✓ legittimi, nel senso che oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
- ✓ compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi.

I dati devono inoltre essere:

- esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
- pertinenti, ovvero, necessari e/o utili per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
- completi, non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di trattare tutti i dati pertinenti per il perseguimento del concreto interesse del soggetto interessato;
- non eccedenti, in senso quantitativo rispetto allo scopo perseguito;
- conservati per un periodo non superiore a quello necessario per gli scopi del trattamento, anche nel rispetto delle disposizioni vigenti in tema di conservazione della documentazione sanitaria. A tal fine si rinvia al prontuario di scarto archivio visibile sul sito aziendale.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Ciascun trattamento deve inoltre avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona e della sua identità personale.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Codice, è necessario provvedere alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile procedere alla regolarizzazione.

Per la violazione delle disposizioni in materia di trattamento dei dati personali il Codice Privacy prevede sanzioni penali (artt. 167 e ss. D. Lgs. n. 196/03) la cui responsabilità resta a carico della singola persona cui l'uso illegittimo dei dati sia imputabile.

In merito alla responsabilità civile si fa rinvio all'art. 15 del Codice privacy il quale dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento.

### **COMPITI PARTICOLARI DEL RESPONSABILE**

Il Responsabile del trattamento dei dati personali deve:

- identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o anonimizzazione dei dati obsoleti;
- provvedere ad informare i soggetti interessati sulle modalità e gli scopi del trattamento, vigilando anche sulla presenza dei cartelli contenenti l'informativa, in tutti i luoghi in cui vengono erogate prestazioni di carattere sanitario, di prevenzione, amministrative, socio-sanitarie, ecc., con la precisazione che questa integra ma non sostituisce l'obbligo di informativa in forma orale o scritta;
- assicurarsi che il trattamento dei dati per lo svolgimento di prestazioni sanitarie finalizzate alla tutela della salute o dell'incolumità fisica dell'interessato, di un terzo o della collettività sia subordinato alla preventiva acquisizione del consenso, salvi i casi di emergenza ed incolumità fisica analiticamente indicati nell'art. 82 del Codice privacy. In caso di trattamento di dati genetici, e in tutti gli altri casi ove sia espressamente previsto, la preventiva acquisizione del consenso deve avvenire obbligatoriamente in forma scritta;

- assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca (art. 100), il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
- adempiere agli obblighi di sicurezza, quali:
  - adottare tutte le preventive misure di sicurezza previste dal Codice Privacy, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31 Codice Privacy);
  - comunicare tempestivamente al Titolare e al Referente aziendale privacy casi di accesso non autorizzato ai dati o di trattamento non consentito, o non conforme alle finalità istituzionali;
- far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti:
  - in particolare, comunicare preventivamente al Titolare l'inizio di ogni attività (trattamento) che deve essere oggetto di notifica al Garante ex art. 37 del Codice Privacy;
  - segnalare al Titolare l'eventuale cessazione di trattamento.
- in merito agli Incaricati, il Responsabile deve:
  - individuare, tra i propri collaboratori, designandoli per iscritto, anche ed eventualmente per qualifica e funzione, gli Incaricati del trattamento, avendo cura di conservare le relative nomine sottoscritte per presa visione;
  - fornire le istruzioni, impartite dal Titolare, cui devono attenersi gli Incaricati nel trattamento dei dati, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati;
  - stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli Incaricati, avendo cura di adottare preventivamente le misure organizzative idonee e impartire le necessarie istruzioni ai fini del riscontro di eventuali richieste di esercizio dei diritti di cui all'art. 7 del Codice Privacy.
- trasmettere le richieste degli interessati all'Ufficio Privacy, ai fini dell'esercizio dei diritti di cui agli artt. 7, 8, 9 e 10 del Codice Privacy;
- collaborare, per quanto di competenza, con il Titolare e con il Referente Privacy per l'evasione delle richieste degli interessati inerenti il trattamento dei dati ai sensi dell'art. 10 del Codice Privacy e delle istanze del Garante per la protezione dei dati personali;

- proporre al Titolare del trattamento dei dati la nomina di soggetti esterni quali Responsabili del trattamento dati in relazione all'affidamento agli stessi di determinate attività, nell'ambito dei compiti istituzionali dell'Azienda;
- collaborare più in generale con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal D. Lgs. 196/2003 e segnalare eventuali problemi applicativi.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali e all'ulteriore documentazione di interesse che potrà essere consultata sul sito aziendale alla voce "privacy".

Il Referente aziendale Privacy, è a disposizione per tutti gli eventuali chiarimenti.



**ESTRATTO INFORMATIVA**

Ai sensi dell'art.13 del D.lgs n° 196 del 30 giugno 2003

*“Codice in materia di protezione dei dati personali”*

Gentile Signore/a,

L'Azienda USL..... La informa su come tratta i Suoi dati sanitari

**I DATI SONO UTILIZZATI PER**

Tutelare la salute e l'incolumità fisica

Condurre ricerche scientifiche e statistiche in forma anonima

Svolgere gli adempimenti amministrativo-contabili anche da parte di altri soggetti pubblici individuati per legge per specifiche finalità

Verificare il gradimento dei servizi e delle prestazioni erogate

Attuare percorsi formativi per operatori sanitari sulla base di specifici accordi

**I DATI RACCOLTI SONO**

Impiegati in modo corretto, nel rispetto del segreto professionale e di ufficio

Trattati sia manualmente che con procedure informatiche anche presso altri

Soggetti all'uopo individuati ed espressamente autorizzati

Conservati con cura, in ambienti idonei e con adeguate misure di sicurezza

Comunicati ad altri solo se previsto dalla legge

**TITOLARE DEL TRATTAMENTO E'**

L'Azienda nella persona del suo legale rappresentante, il Direttore Generale.

L'Azienda ha inoltre nominato i Responsabili del trattamento che, a loro volta, hanno designato gli Incaricati al trattamento dei dati. L'elenco dei Responsabili è disponibile nel sito aziendale

**PER TRATTAMENTO SI INTENDE (art. 4 D. Lgs 196/03)**

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici (raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione o distruzione di dati, anche se non registrati in una banca dati).

**MEDIANTE RICHIESTA SCRITTA ALL'UFFICIO PRIVACY (indirizzo mail)**

Lei può esercitare i propri diritti (art. 7 D.Lgs 196/03) quali:

- conoscere se e come i Suoi dati sono utilizzati
- conoscere il nome del responsabile del trattamento
- conoscere a chi sono comunicati i Suoi dati
- avere ogni ulteriore informazione sul trattamento dei dati

**PRESSO L'UFFICIO PRIVACY, INOLTRE, LEI PUO':**

- Presentare segnalazioni sul mancato rispetto della normativa in tema di “privacy”
  - Esprimere l'eventuale dissenso al trattamento di tutti o in parte dei dati forniti.
- In tal caso Le ricordiamo che il trattamento dei suoi dati è condizione necessaria per consentire all'Azienda di erogare al meglio i propri servizi.

Il Regolamento aziendale Privacy, il modulo per la richiesta ed ulteriori informazioni, sono reperibili nel sito aziendale e presso l'Ufficio Relazioni con il Pubblico (URP)

Azienda \_\_\_\_\_ Via \_\_\_\_\_ Città \_\_\_\_\_ [www.uslxx.toscana.it](http://www.uslxx.toscana.it)  
privacy@usl\_\_\_\_\_ .it – pec(protocollo)@\_\_\_\_\_ .it Numero Verde 000.000.000

**ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

Il/La sottoscritto/a \_\_\_\_\_  
nato/a a \_\_\_\_\_ il \_\_\_\_\_,  
esercita con la presente richiesta i suoi diritti di cui all'articolo 7 del Codice in materia di protezione  
dei dati personali (d.lgs. 30 giugno 2003, n. 196):

**Accesso ai dati personali** (art. 7, comma 1, del Codice)

Il sottoscritto intende accedere ai dati che lo riguardano e precisamente:

- ☐ chiede di confermarli l'esistenza o meno di tali dati, anche se non ancora registrati,  
e/o  
☐ chiede di comunicargli i medesimi dati in forma intelligibile (art. 10 del Codice).

*La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):*

\_\_\_\_\_  
\_\_\_\_\_

**Richiesta di conoscere alcune notizie sul trattamento** (art. 7, comma 2, del Codice)

Il sottoscritto chiede di conoscere:

- ☐ l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);  
☐ le finalità del trattamento dei dati che lo riguardano;  
☐ le modalità del medesimo trattamento;  
☐ la logica applicata al trattamento effettuato con strumenti elettronici;  
☐ gli estremi identificativi del titolare del trattamento (ovvero della pubblica amministrazione, della persona giuridica pubblica o privata, dell'associazione od organismo che li tratta);  
☐ gli estremi identificativi del/i responsabile/i del trattamento (nel caso in cui siano designati ai sensi dell'art. 29 del Codice);  
☐ i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o di incaricati o di rappresentante designato nel territorio dello Stato;  
☐ gli estremi identificativi del rappresentante del titolare nel territorio dello Stato (se designato ai sensi dell'art. 5 del Codice).

*La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):*

\_\_\_\_\_  
\_\_\_\_\_

### **Richiesta di intervento sui dati**

(art. 7, comma 3, del Codice) (Barrare solo le caselle che interessano)

Il sottoscritto chiede di effettuare le seguenti operazioni:

- ☐ aggiornamento dei dati;
- ☐ rettificazione dei dati;
- ☐ integrazione dei dati;
- ☐ cancellazione dei dati trattati in violazione di legge  
(compresi quelli di cui non è necessaria la conservazione);
- ☐ trasformazione in forma anonima dei dati trattati in violazione di legge  
(compresi quelli di cui non è necessaria la conservazione);
- ☐ blocco dei dati trattati in violazione di legge  
(compresi quelli di cui non è necessaria la conservazione);
- ☐ attestazione che tale intervento sui dati è stato portato a conoscenza, anche per quanto riguarda il suo contenuto, di coloro ai quali i dati sono stati comunicati o diffusi.

La presente richiesta riguarda *(indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento)*:

---

---

### **Opposizione al trattamento per fini pubblicitari**

(art. 7, comma 4, del Codice)

- ☐ Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

### **Opposizione al trattamento per motivi legittimi**

(art. 7, comma 4, del Codice)

- ☐ Il sottoscritto si oppone al trattamento dei dati per i seguenti motivi legittimi:

---

---

---

La presente richiesta riguarda *(indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento)*:

---

---

---

Il sottoscritto si riserva di rivolgersi all'autorità giudiziaria o al Garante con ricorso (artt. 145 ss. del Codice) se entro 15 giorni dal ricevimento della presente istanza non perverrà un riscontro idoneo.

**Recapito per la risposta:**

☐ Indirizzo postale: \_\_\_\_\_  
Via/Piazza \_\_\_\_\_  
Comune \_\_\_\_\_  
Provincia \_\_\_\_\_ Codice postale \_\_\_\_\_

**oppure**

☐ e-mail: \_\_\_\_\_

**oppure**

☐ telefax: \_\_\_\_\_

**oppure**

☐ telefono\*: \_\_\_\_\_

**Eventuali precisazioni**

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

---

---

---

---

---

---

Estremi di un documento di riconoscimento\*\*:

---

\_\_\_\_\_  
(Luogo e data)

\_\_\_\_\_  
(Firma)

\* Le richieste in esame e la relativa risposta possono essere anche orali. Tuttavia, se l'interessato si rivolge al Garante con un ricorso, occorre allegare copia della richiesta rivolta al titolare (o al responsabile, se designato) del trattamento.

\*\* Esibire o allegare copia di un documento di riconoscimento, se l'identità del richiedente non è accertata con altri elementi.