



**AZIENDA ULSS N. 16  
PADOVA**

**AZIENDA OSPEDALIERA  
PADOVA**



# **MANUALE DELLA PRIVACY**

**Allegato n. 3)** alla deliberazione n. 231 del 30.3.2006 dell'Azienda Ospedaliera di Padova.

# INDICE

**PREMESSA**..... p. 3

## **CAPITOLO 1 - Elementi introduttivi sul d. lgs. 196/2003 (Codice in materia di protezione dei dati personali)**

- 1.1. Oggetto del codice della privacy e ambito di applicazione ..... p. 4
- 1.2. La definizione di trattamento di dati personali ..... p. 5
- 1.3. Le diverse tipologie di dati personali: dati sensibili e giudiziari, dati comuni e dati semi-sensibili ..... p. 6
- 1.4. I principi generali in tema di trattamento dei dati personali..... p. 7
- 1.5. I soggetti che effettuano il trattamento dei dati personali: titolare, responsabili e incaricati..... p. 9
- 1.6. Gli adempimenti previsti dal codice della privacy per i soggetti pubblici..... p. 10
- 1.7. Sanzioni previste dal Codice della privacy..... p. 13

## **CAPITOLO 2 - Istruzioni per i responsabili e gli incaricati del trattamento dei dati personali.**

- 2.1. Istruzioni di carattere generale per tutti i responsabili e gli incaricati..... p. 16
- 2.2. Istruzioni specifiche per i responsabili e gli incaricati delle strutture che erogano prestazioni sanitarie (prevenzione, diagnosi, cura e riabilitazione dello stato di salute) ..... p. 17
- 2.3. Istruzioni specifiche per gli addetti alla manutenzione e alla gestione degli strumenti elettronici e delle attrezzature elettromedicali ..... p. 19
- 2.4. Istruzioni specifiche per il corretto uso e la sicurezza degli strumenti e per la protezione dei dati personali ..... p. 20
- 2.5. Istruzioni per il corretto trattamento dei dati su supporto cartaceo..... p. 24

## **ALLEGATI :**

- Modulistica per l'informativa e per l'acquisizione del consenso.

## PREMESSA

Già a partire dall' applicazione della prima legge sulla Privacy (L. 675/96), l' Azienda ULSS 16 e l'Azienda Ospedaliera di Padova avevano avvertito una forte responsabilità e impegno per adeguare le proprie strutture e l'organizzazione delle attività istituzionali alla normativa sulla tutela del diritto alla riservatezza dei propri utenti, dipendenti, collaboratori e fornitori.

Con l'entrata in vigore del D.Lgs 196/2003 "Codice in materia di protezione dei dati personali" – che ha abrogato la precedente normativa – l'Azienda ULSS 16 e l'Azienda Ospedaliera, consapevoli che nella particolare realtà in cui opera un'azienda sanitaria sono quotidianamente trattati una pluralità di dati d'estrema delicatezza come quelli riguardanti la salute dei cittadini, intendono intensificare l'impegno per garantire la protezione dei dati personali e per evitare che un loro uso scorretto possa danneggiare o ledere i diritti, le libertà fondamentali e la dignità delle persone interessate.

A partire dalla convinzione che al rispetto della privacy si può pervenire non solo attuando gli adempimenti formali previsti dalla normativa, ma anche e soprattutto attraverso un graduale e continuo percorso informativo / formativo dei propri dipendenti e collaboratori, finalizzato a far maturare e crescere la cultura della privacy, si è ritenuto opportuno predisporre questo strumento contenente oltre che alcuni indispensabili elementi introduttivi sul D.Lgs. 196/2003, meglio conosciuto come Codice della privacy, anche le necessarie ed opportune istruzioni di carattere generale e specifico alle quali tutti i responsabili e gli incaricati dei trattamenti dei dati personali, eseguiti nell'ambito delle competenze formalmente assegnate, devono quotidianamente attenersi.

Questo manuale rappresenta un primo intervento di informazione e formazione di base - rivolto a tutti i propri dipendenti e collaboratori - in materia di protezione dei dati personali al quale seguiranno, già a partire dall'anno in corso, una serie di interventi formativi di approfondimento per ognuna delle categorie omogenee (medici, infermieri, amministrativi, tecnici, ecc.) di responsabili ed incaricati dei trattamenti dei dati personali.

Il coordinamento di tutte le attività riguardanti l'applicazione della normativa in materia di privacy è stato affidato al Direttore della Struttura Complessa Interaziendale Amministrazione Dott. Franco Cardin (tel. 1540 / fax 1526 / e-mail franco.cardin@sanita.padova.it) al quale ci si può rivolgere per ogni necessità riguardante sia gli aspetti normativi che operativi.

Il Direttore Generale  
Azienda Ulss 16  
Dott. Fortunato RAO

Il Direttore Generale  
Azienda Ospedaliera  
Dott. Adriano CESTRONE

# CAPITOLO 1 - Elementi introduttivi sul D. lgs. 196/2003 “Codice in materia di protezione dei dati personali”

## 1.1. Oggetto del codice della privacy e ambito di applicazione.

Con il d. lgs. 30 giugno 2003, n. 196, è stato adottato il codice in materia di protezione dei dati personali (meglio noto come codice della privacy) ed è stata abrogata la legge 675/96 e i decreti modificativi e integrativi.

Oggetto del codice della privacy è la disciplina del trattamento dei dati personali, che deve svolgersi nel rispetto dei diritti e delle libertà fondamentali, con particolare riferimento alla riservatezza, all'identità personale e al **diritto alla protezione dei dati personali**.

Il codice, di conseguenza, non disciplina la tenuta delle banche dati o degli archivi, ma detta una serie di regole per il corretto trattamento dei dati personali.

Ogni trattamento di dati personali consiste in un rapporto che si instaura tra titolare e interessato:

- **titolare del trattamento** è la persona fisica, persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo, cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nel caso di specie titolare del trattamento è l'azienda sanitaria come entità nel suo complesso;
- **interessato al trattamento**: è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Il diritto alla riservatezza è definito come il diritto ad essere lasciato solo: è un diritto assoluto alla protezione della propria sfera personale e familiare, con possibilità dell'interessato di scegliere e disporre se fare conoscere a terzi i propri dati personali e, in caso affermativo, in quale contesto e con quali forme.

Anche a causa dell'evolversi delle tecnologie informatiche e telematiche, il concetto di privacy si è evoluto da “diritto ad essere lasciato solo” a “diritto alla protezione e al controllo sul trattamento dei propri dati personali svolto da terzi”.

Attualmente il codice della privacy riconosce, a ciascuna persona interessata al trattamento, il diritto alla protezione dei propri dati personali, che si sostanzia da un lato nell'obbligo per il titolare del trattamento di adottare misure di sicurezza a protezione dei dati personali e, dall'altro, nella facoltà per ciascun interessato di poter esercitare i diritti previsti dall'art. 7 del codice della privacy ( diritto di accesso, diritto di informativa, diritto di opporsi in tutto o in parte al trattamento).

## 1.2. La definizione di trattamento di dati personali

L'articolo 4 del codice della privacy definisce il **trattamento** come “*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, 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, anche se non registrati in una banca di dati*”.

Quest'ultimo inciso è stato opportunamente aggiunto nel codice (non era presente nella legge 675/96) al fine di fugare possibili interpretazioni (in molti casi fuorvianti), che portavano ad eludere l'applicazione della normativa considerata.

Va richiamata, quindi, la definizione di **banca dati**: con tale espressione si intende “qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti”. Ciò che caratterizza la nozione di banca dati, ovvero quella di archivio - intendendosi con quest’ultima espressione la raccolta cartacea - è l’organizzazione dei dati al fine di favorire la loro ricerca e reperimento.

Quanto alle modalità di svolgimento delle operazioni considerate, il codice trova applicazione non solo nel caso in cui siano utilizzati strumenti elettronici, ma anche strumenti non automatizzati (ad esempio il cartaceo): con l’espressione **strumento elettronico** ci si riferisce agli “*elaboratori, ai programmi per elaboratori e a qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento*”.

Con il termine trattamento si comprendono, pertanto, tutte le operazioni possibili che possono avere ad oggetto dati personali. Considerando che trattasi comunque di un processo - caratterizzato da una serie di fasi finalizzate al raggiungimento di uno scopo o risultato finale - è possibile schematizzarne le seguenti tre fasi:

- a) **l’input**, costituito dalla raccolta del dato personale: questa potrà avvenire utilizzando, come detto, strumenti elettronici (avremo molto spesso una coincidenza tra raccolta e registrazione) ovvero attraverso uno sportello (pensiamo agli utenti che si rivolgono ad uno sportello di accettazione) con un momento successivo dedicato alla registrazione dei dati personali raccolti, sia elettronicamente, sia su supporto cartaceo. In questa fase è richiesta una attenta verifica dell’esattezza dei dati, anche e soprattutto ove i dati siano riferiti a terzi (è il caso che si verifica di sovente ad esempio per le autocertificazioni del reddito ovvero con riferimento ad altri servizi che possono essere richiesti all’azienda);
- b) vi è poi la fase del **processo di trattamento interno**, caratterizzata dal complesso di operazioni richiamate in precedenza, che possono essere distinte in statiche (registrazione, organizzazione e conservazione) e in dinamiche, che sono le restanti. Questa distinzione rileva soprattutto con riferimento all’aggiornamento dei dati trattati: fermo l’obbligo di dover verificare l’esattezza dei dati al momento della raccolta (cfr. articolo 11, comma 1 lettera c), il codice prevede, se necessario, anche l’aggiornamento, con ciò dovendosi ritenere che tale operazione è necessaria solo ove si svolgano operazioni dinamiche;
- c) infine, il processo di trattamento può prevedere anche la **cd. fase di out-put**, che consiste nel trasferire dati personali a soggetti terzi, diversi dall’interessato. Questa può consistere nella **comunicazione o diffusione dei dati**: queste due operazioni presuppongono che rispetto al rapporto bilatero esistente tra titolare del trattamento (l’azienda) e l’interessato (l’utente, un dipendente, una ditta che partecipa ad un appalto) si inserisce un terzo soggetto, che può avere conoscenza dei dati personali riferiti a quest’ultimo o sia destinatario degli stessi. La differenza tra comunicazione e diffusione risiede, peraltro, nella determinazione o meno del soggetto destinatario dell’operazione considerata: ove il soggetto sia determinato avremo una **comunicazione di dati**, che consiste nel “*dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, dal rappresentante del titolare, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*”. Viceversa, nel caso in cui il soggetto che conosce i dati non sia determinato, avremo una **diffusione di dati** (si pensi all’inserimento dei dati in Internet, ovvero alla loro pubblicazione sul BUR o in Gazzetta Ufficiale,...). La distinzione tra le due operazioni considerate rileva soprattutto con riferimento alla previsione del **divieto di diffusione dei dati idonei a rivelare lo stato di salute**, che riguarda sia i soggetti privati (ai sensi dell’articolo 26, comma 5 del codice), sia i soggetti pubblici (cfr. articolo 22, comma 8 del codice). La violazione di tale obbligo potrà avere conseguenze sia di natura penalistica, sia civilistica.

### 1.3. Le diverse tipologie di dati personali: dati sensibili e giudiziari, dati comuni e dati semi-sensibili.

Per “**dato personale**” si intende “*qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*”.

Il codice presenta inoltre una novità, rispetto alla legge 675/96, che riguarda la nozione di “**dato identificativo**”, che è definito come il dato personale che permette l’identificazione diretta dell’interessato.

La distinzione tra dato personale (in generale) e dato identificativo (in particolare) ha rilievo soprattutto con riferimento a quanto previsto dall’articolo 3 del codice, che prevede il **principio di necessità**, che costituisce una novità assoluta rispetto alla legge 675/96: “*i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l’utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati personali od opportune modalità che permettano di identificare l’interessato solo in caso di necessità*”.

La nozione di dato personale, peraltro, è molto ampia tanto da ricomprendere, come chiarito dal Garante per la protezione dei dati personali, qualunque informazione comunque riferita ad un soggetto determinabile: si pensi, tra i casi considerati, alle registrazioni audiovisive (l’installazione di videocamere, che siano idonee a identificare i soggetti che circolano in una certa area o che accedano ad esempio ad un Dipartimento), ovvero alle audioregistrazioni o videoregistrazioni (che possono essere utilizzate in sede anamnestica o diagnostica per immagini).

Nell’ambito della categoria dei dati personali, possono essere distinte quattro famiglie di informazioni:

- ÿ i **dati sensibili**: sono 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*”. Tali informazioni costituiscono da sempre il cd. nocciolo duro della tutela della riservatezza, per i quali esistono obblighi di tutela della riservatezza con specifico riferimento ai dati di salute (si pensi alla tutela del lavoratore dipendente ai sensi degli articoli 5 e 8 della legge 300/1970 – cd. Statuto dei lavoratori – ovvero alla legge sull’interruzione volontaria della gravidanza (IVG), o ancora alla tutela del soggetto sieropositivo ai sensi della legge 135/90 o al diritto all’anonimato per i tossicodipendenti (DPR 309/1990).
- ÿ La principale novità che riguarda le disposizioni del codice rispetto alle leggi settoriali adottate in precedenza (e richiamate brevemente) consiste in ciò: in precedenza la tutela era prevista con riferimento al soggetto che procedeva al trattamento di tali informazioni (si pensi al medico e all’obbligo del segreto professionale) ovvero alla natura soggettiva (dipendente, tossicodipendente, sieropositivo) o al luogo in cui tali informazioni venivano trattate (struttura sanitaria, luoghi di lavoro); attualmente, la protezione è di carattere oggettivo, avendo riguardo al solo contenuto dell’informazione a prescindere dal soggetto o dal luogo specificamente dedicato, in cui tali informazioni sono raccolte o trattate.
- ÿ Ciò ha portato alla oggettivizzazione delle forme di tutela dei dati personali, che sono nel codice della privacy oggetto di tutela in sé. Questo giustifica, altresì, la scelta del

legislatore di definire il dato sensibile (cfr. articolo 4, comma 1 lettera d) del codice) non utilizzando l'espressione "dati riferiti, concernenti, riguardanti", ma una locuzione di portata ed efficacia più ampia e onnicomprensiva come "dati idonei a rivelare ...".

- ÿ Ciò determina che non è possibile in termini generali ed astratti qualificare un'informazione come di carattere sensibile dovendosi sempre valutare le connessioni esistenti tra due diversi dati e informazioni, che siano idonei a rivelare stati, fatti o qualità di natura sensibile, nei limiti, ovviamente, della ragionevolezza. Pensiamo, ad esempio, alla busta paga, che contiene dati di natura economica, di per sé non aventi natura sensibile; tuttavia, un'indennità percepita da un lavoratore per un figlio portatore di handicap, pur essendo un'informazione di natura economica è idonea a rivelare lo stato di salute di un soggetto, per cui può qualificarsi come dato sensibile. Altre volte è la finalità del trattamento che da sola può essere idonea a determinare la natura dei dati, altrimenti neutri (ad esempio attività ricreative, organizzazione di soggiorni estivi per soggetti che hanno problemi di salute);
- ÿ una seconda categoria di dati è rappresentata dai cd. **dati giudiziari**, che sono quelle informazioni idonee a rivelare una serie di provvedimenti di carattere giurisdizionale di natura penale: questi sono espressamente previsti ed individuati dall'articolo 4, comma 1 lettera e) del codice. Il riferimento è ai dati del casellario giudiziale – ad esclusione del provvedimento di dichiarazione di fallimento e di quello di interdizione e inabilitazione – all'anagrafe delle sanzioni amministrative dipendenti da reato e relativi carichi pendenti, alla qualità di indagato o di imputato;
- ÿ al di fuori di queste due categorie considerate, ci sono i **dati cd. comuni**, la cui portata si ricava in via residuale e per esclusione, essendo i dati riferiti ad un soggetto identificato o identificabile, che non siano idonee a rivelare gli stati, fatti o qualità contemplati dal legislatore con riferimento alle categorie dei dati cd. particolari (sensibili o giudiziari). Per questi occorre considerare che la normativa in materia di privacy si applica in ogni caso, con alcune differenziazioni sotto il profilo delle forme di legittimazione e per quanto concerne le misure di sicurezza;
- ÿ vi è poi una ulteriore classe di dati, definiti **quasi-sensibili o semi-sensibili**, che comprende quei dati che pur non essendo di natura sensibile o giudiziaria, qualora siano trattati possono comportare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura stessa dei dati, alle modalità del trattamento o agli effetti che può determinare. In tal caso, ai sensi dell'articolo 17 del codice, il Garante può prescrivere misure e accorgimenti specifici: è una categoria aperta di informazioni, costituente una sorta di valvola di sicurezza del sistema di protezione dei dati personali disegnato dal legislatore, che costituisce elemento caratterizzante la natura rimediale della normativa in tema di privacy e l'oggettivizzazione delle forme di tutela considerate.

#### 1.4. I principi generali in tema di trattamento dei dati personali.

Il codice della privacy, mutuando dalla normativa comunitaria (in particolare dalla direttiva 95/46/CE), prevede una serie di principi generali destinati ad incidere con forza innovativa sull'attività di trattamento dei dati personali.

Il primo e fondamentale principio in tema di trattamento dei dati è il **principio di scopo**. L'articolo 11, comma 1 lettera b) del codice dispone che i dati possono essere raccolti e registrati per "*scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi*". Ciò comporta l'abbandono della precedente filosofia, tanto cara a qualsiasi operatore, di raccogliere dati personali perché comunque utili per l'esercizio di una attività futura.

Ogni trattamento, secondo il principio testé richiamato, deve fondarsi su di una **finalità**:

- a) **determinata** (lo scopo deve essere definito e delimitato, al fine di favorire un controllo sulla portata delle operazioni effettuabili). Nel caso dei soggetti pubblici è la stessa legge che lo determina in considerazione del fatto che le pubbliche amministrazioni agiscono sempre per finalità istituzionale, per cui l'agire amministrativo non è mai libero nello scopo;
- b) **esplicita**: tale criterio valutativo richiede la necessaria trasparenza del proprio agire, con ciò dovendo avere riguardo agli obblighi di informativa all'interessato, espressamente previsti dal codice della privacy (cfr. articolo 13).
- c) **legittima**: significa che nel procedere al trattamento non solo non si potranno perseguire scopi illeciti (si pensi alla comunicazione di dati personali a società di marketing interessate a vendere beni o servizi alle imprese - utenti dei servizi aziendali), ma occorrerà altresì rispettare le previsioni del codice e delle leggi specifiche di settore.

L'importanza della determinazione dello scopo del trattamento rileva anche con riferimento al cd. **diritto all'oblio**, espressamente contemplato dalla normativa in tema di privacy, ai sensi dell'articolo 11, comma 1 lettera e).

Con quest'ultima espressione si intende che i dati possono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Se da un lato vi è la necessità di perseguire uno scopo (che abbia le caratteristiche richiamate in precedenza) per poter iniziare un'attività di trattamento, dall'altro il raggiungimento delle finalità costituisce circostanza da valutarsi ai fini della conservazione dei dati (in chiaro ossia in forma identificativa dell'interessato) raccolti e registrati, che una volta raggiunto lo scopo dovranno essere trasformati in forma non identificativa.

Occorrerà, tuttavia, verificare quali siano i tempi e gli obblighi di conservazione specificamente previsti da parte del legislatore o ritenuti comunque congrui per le finalità del trattamento svolte in ambito pubblico: le scritture contabili, ad esempio, devono essere conservate per dieci anni; la documentazione amministrativa in molti casi acquista valore archivistico e deve essere conservata negli archivi storici trascorsi quaranta anni dalla conclusione degli affari, cui si riferisce, e per poter essere distrutta (il cd. scarto) occorre l'autorizzazione della Sovrintendenza Archivistica competente. In altri casi, esigenze di tutela in sede giudiziaria possono legittimare la conservazione per fini probatori della documentazione e quindi dei dati ivi contenuti per i tempi di prescrizione ordinaria ovvero di decadenza.

Strettamente connesso al principio di scopo appare essere un secondo limite fondamentale, riguardante la **proporzionalità** e l'**adeguatezza** dei dati personali trattati rispetto agli scopi, che si estrinseca nell'obbligo di procedere alla raccolta e al trattamento di dati **pertinenti, completi** e non **eccedenti**, rispetto alle finalità del trattamento (cfr. articolo 11, comma 1 lettera d) del codice).

Questo limite di carattere generale richiede una assoluta attenzione e cautela non solo per quanto riguarda la fase della registrazione dei dati e dell'elaborazione ed utilizzo degli stessi, con specifico riferimento all'attività amministrativa dell'ente, ma soprattutto per quanto concerne la comunicazione dei dati a terzi all'esterno dell'ente.

Il limite della proporzionalità dei dati, che, come detto, riguarda la necessità di verificare la pertinenza, non eccedenza e completezza degli stessi, consiste in un limite da valutarsi *a priori* (in termini astratti), ma anche *a posteriori* in occasione dello svolgimento della propria attività in modo concreto e specifico, relativamente all'ambito e al contesto.

Con riferimento al trattamento dei dati sensibili o giudiziari, i soggetti pubblici possono procedere al trattamento dei dati considerati solo ove ciò sia indispensabile rispetto agli scopi da perseguire in concreto, secondo quanto previsto dall'articolo 22, comma 3 del codice. Ciò comporta anche una serie di obblighi di controllo e di monitoraggio continuo secondo quanto previsto dal comma 5 del medesimo articolo ivi considerato.

Altro profilo fondamentale previsto dal codice è rappresentato dal cd. **principio del “prior checking”**, secondo cui è indispensabile l'adozione di misure differenziate di tutela e protezione dei dati personali a seconda della natura dei dati oggetto di trattamento.

Sono da inquadrare in questa ottica le previsioni aventi ad oggetto l'adozione di misure di sicurezza, ovvero quelle disciplinanti il potere del Garante di dettare una serie di criteri per evitare i rischi specifici connessi al trattamento dei dati diversi da quelli di natura sensibile o giudiziaria. Direttamente connesso al principio del prior checking è il principio di sicurezza dei dati personali, che si estrinseca nell'obbligo dell'adozione di misure di sicurezza sia di natura idonea, sia di carattere minimo.

### **1.5. Soggetti che effettuano il trattamento dei dati personali: titolare, responsabili e incaricati**

Il trattamento dei dati personali è caratterizzato dalla presenza, dal lato attivo, del titolare del trattamento e, dal lato passivo, dell'interessato.

Dal lato attivo, come detto, la nostra normativa, su influsso specifico della direttiva comunitaria numero 95/46, contempla tre diverse figure, che possono coesistere nell'ambito di un processo di trattamento: **il titolare, il responsabile e l'incaricato** del trattamento.

Si è in precedenza richiamata la definizione di titolare del trattamento. In particolare, l'articolo 28 del codice della privacy dispone che quando il trattamento è effettuato da una pubblica amministrazione titolare è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza, come detto in precedenza. Ciò comporta che nel nostro caso specifico, **l'Azienda ULSS 16 e l'Azienda Ospedaliera sono ognuna titolare del trattamento come entità**, non essendo corretto qualificare i rispettivi Direttori Generali, che pur le rappresentano legalmente, come titolari del trattamento.

La scelta adottata dal legislatore della privacy è, come si può constatare, profondamente differente rispetto a quella della normativa in tema di sicurezza nei luoghi di lavoro (ad esempio il d. lgs. 626/94), ove vi è il riferimento alla figura del datore di lavoro definito come persona fisica.

Nelle organizzazioni complesse, come può essere quella di un'azienda sanitaria, vi è la facoltà di provvedere alla designazione di uno o più **responsabili del trattamento** che, come dispone l'art. 29 del codice devono essere individuati *“tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza”*. Ai responsabili, se designati, il titolare deve affidare compiti analiticamente specificati per iscritto, nonché impartire adeguate istruzioni.

L'art. 30 del codice privacy prevede, inoltre, che *“le operazioni di trattamento possono essere effettuate solo da **incaricati** che operano sotto la diretta autorità del titolare o del responsabile attenendosi alle istruzioni impartite”*.

Vi è, di conseguenza, l'obbligo di procedere alla designazione, sempre per iscritto, in qualità di incaricati, di tutte le persone fisiche che a vario titolo sono preposte allo svolgimento delle operazioni di trattamento per conto del titolare – cioè dell'azienda – nonché impartire loro adeguate istruzioni.

Queste previsioni di carattere organizzativo sono state applicate sia nell'Azienda ULLS 16 che nell'Azienda Ospedaliera di Padova designando, con delibera dei rispettivi Direttori Generali:

- ÿ quali **responsabili dei trattamenti**, effettuati nell'ambito delle funzioni e delle competenze formalmente attribuite ad ogni singola struttura, tutti i Direttori di Struttura Complessa, i Responsabili di Struttura Semplice e i Responsabili dei Servizi di Staff;
- ÿ quali **incaricati dei trattamenti**, effettuati nell'esercizio delle mansioni svolte nell'ambito della struttura alla quale sono stati formalmente assegnati, tutti i dipendenti e tutte le persone fisiche che a vario titolo svolgono temporaneamente attività all'interno di una delle varie strutture aziendali (specializzandi, frequentatori, tirocinanti, collaboratori, stagisti).

Con le predette deliberazioni sono stati inoltre approvati, sia l'elenco analitico dei compiti affidati ai responsabili, nonché il presente Manuale della Privacy che nel capitolo 2) riporta le necessarie ed opportune istruzioni, alle quali tutti i dipendenti e collaboratori – siano essi designati responsabili o incaricati – devono scrupolosamente attenersi nelle operazioni di trattamento dei dati.

## 1.6. Gli adempimenti previsti dal codice della privacy per i soggetti pubblici.

1) L'art. 13 del codice della privacy prevede che l'interessato o la persona presso la quale sono raccolti i dati siano previamente informati oralmente o per iscritto circa :

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
- gli estremi identificativi del titolare e, se designato, anche quelli del responsabile.

Come risulta evidente l'**informativa**, che costituisce un obbligo ascritto alla trasparenza dei trattamenti, deve:

- a) essere fornita all'interessato al momento della raccolta del dato personale;
- b) ove la raccolta riguardi dati personali forniti da un soggetto diverso dall'interessato (si pensi all'autocertificazione del reddito familiare, in cui il dichiarante fornisce dati di interessati diversi dalla sua persona), l'informativa deve essere data sia a chi fornisce i dati (al momento della raccolta, come detto), sia all'interessato (a quest'ultimo non più tardi del momento della registrazione ovvero della prima comunicazione dei dati). L'obbligo di informare la persona interessata nel caso di raccolta di dati presso terzi è escluso nel caso in cui la raccolta di dati presso terzi sia prevista come obbligo previsto da legge, regolamento, normativa comunitaria ovvero quando il trattamento è effettuato ai fini dello svolgimento delle investigazioni difensive di cui alla legge 397/2000 o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento (cfr. articolo 13, comma 5 del codice della privacy);
- c) nel caso di trattamento di dati sensibili e giudiziari, i soggetti pubblici devono fare espresso riferimento nell'informativa alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati considerati (ai sensi dell'articolo 22, comma 2 del codice della privacy);
- d) può essere fornita anche in forma orale; a seconda delle modalità di raccolta del dato e del rapporto con gli interessati, quindi, può essere fornita attraverso manifesti (nel caso di rapporti di sportello o di sale per l'attesa della prestazione), ovvero apponendola in calce alla modulistica per le autocertificazioni, o inserendola

- nei bandi (nel caso di selezioni pubbliche), ovvero in calce alla modulistica predisposta per la presentazione di richieste di prestazioni o servizi;
- e) l'informativa può essere fornita anche dall'incaricato del trattamento;
- f) l'omessa informativa o la sua inidoneità sono condotte sanzionate ai sensi dell'articolo 161 del codice della privacy che prevede la sanzione amministrativa del pagamento di una somma da tremila a diciottomila euro o, nei casi di dati sensibili o giudiziari, di una somma da cinquemila a trentamila euro.

Al fine di facilitare ed omogeneizzare tale importante adempimento da parte di tutti i responsabili dei trattamenti si riportano in allegato al presente manuale gli schemi delle varie tipologie di informative – predisposte per ognuna delle categorie di interessati dai quali si rende necessario acquisire dati durante l'esercizio delle diverse funzioni istituzionali – precisando che le stesse verranno fornite anche in formato elettronico in modo da consentire non solo l'eventuale necessaria personalizzazione ma anche di poter scegliere una delle diverse modalità pratiche utilizzabili per fornirle oralmente o per iscritto agli interessati.

**2) Uno specifico adempimento, previsto dall'art. 76 del codice della privacy, per tutti gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, è quello di acquisire il **consenso dell'interessato** ogni volta si debbano trattare i suoi dati personali idonei a rivelare lo stato di salute.**

Il consenso dell'interessato deve essere obbligatoriamente acquisito:

- ÿ quando il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;
- ÿ quando il trattamento dei dati idonei a rivelare lo stato di salute è finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico;

Nella prima ipotesi, il consenso riguarda l'erogazione delle prestazioni di prevenzione, diagnosi, cura e riabilitazione e deve essere manifestato previa informativa ai sensi dell'art. 13 del codice della privacy.

Con riferimento alla seconda ipotesi, va ricordato che il consenso dell'interessato non deve essere richiesto quando la ricerca:

- è prevista da un'espressa disposizione di legge che prevede specificamente il trattamento;
- rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'art. 12-bis del d. lgs. 502/1992 e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'articolo 39 del codice.

Il consenso non è, inoltre, necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante, anche con provvedimento ad efficacia generale.

Il consenso deve essere:

- ÿ **espresso liberamente**, ossia senza costrizioni e rispettando l'autodeterminazione informativa dell'interessato, con la conseguenza che, salvo lo stato di necessità per la tutela della salute dell'interessato, in caso di soggetto capace di intendere e di volere che negasse il consenso al trattamento, non si potrebbe procedere nel trattamento dei suoi dati di salute, con la conseguenza di vedere preclusa l'assistenza sanitaria;
- ÿ **manifestato in forma specifica**, per cui non può dedursi da comportamenti impliciti o concludenti da parte dell'interessato, occorrendo una manifestazione specifica a tal riguardo.

Quanto alla forma, si segnala un'importante novità introdotta dal codice della privacy: mentre in precedenza, infatti, era necessario il consenso in forma scritta, l'art. 81 del codice dispone che il consenso può essere manifestato anche in forma orale, purché sia documentato con annotazione.

Con tale previsione si riconosce un potere dichiarativo in capo all'operatore incaricato della raccolta del consenso e dell'annotazione della manifestazione di volontà (consenso), a seguito della quale l'azienda è autorizzata al trattamento dei dati di salute. L'effetto che consegue all'annotazione del consenso - manifestato in forma orale - è l'inversione dell'onere della prova, per cui nel caso di contestazione è l'interessato che deve provare di non aver manifestato in precedenza il consenso al trattamento dei propri dati.

L'Azienda ULSS 16 e l'Azienda Ospedaliera prevedono di utilizzare diverse forme di raccolta e di annotazione del consenso. Oltre alla forma scritta, da utilizzare per esempio nel caso di ricovero, mediante l'utilizzo di apposito modulo da compilare a cura dell'incaricato e da inserire in cartella clinica, sarà prossimamente possibile annotare la raccolta del consenso inserendo direttamente un segno di spunta (un flag) in un apposito campo del data-base aziendale, relativo all'anagrafe degli assistiti.

Infine, quanto alla legittimazione, va sottolineato che il consenso deve essere manifestato dall'interessato, maggiore di età, non interdetto e capace di intendere o di volere.

Per i diversi casi di incapacità o di impossibilità, il codice della privacy dispone la legittimazione di uno dei seguenti soggetti:

- a) esercente la potestà, nel caso di minore di età o di persona interdetta o soggetta ad amministrazione di sostegno;
- b) familiare, prossimo congiunto o convivente (tutti posti sullo stesso piano) per le ipotesi di impossibilità fisica o di incapacità di intendere o di volere dell'interessato;
- c) in via residuale, il responsabile della struttura presso cui dimora l'interessato, in assenza dei soggetti indicati alla lettera b).

**3) un altro importante adempimento riguarda l'obbligo di riscontrare le istanze presentate dall'interessato, aventi ad oggetto l'esercizio dei diritti di cui all'articolo 7 del codice.**

Con queste istanze, l'interessato può esercitare:

- a) **il diritto di accesso**, che consiste nella facoltà dell'interessato di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e la loro comunicazione in forma intelligibile. Inoltre, l'interessato può chiedere l'indicazione dell'origine dei dati, delle finalità e modalità di trattamento, della logica e degli estremi identificativi del titolare e del responsabile (trattasi degli elementi costituenti il contenuto dell'informativa, da fornire ai sensi dell'articolo 13);
- b) **poteri di natura inibitoria** che consistono nella possibilità per l'interessato di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati (quest'ultima è una estrinsecazione del cd. diritto all'oblio, di cui si è detto in precedenza, previsto dall'articolo 11, comma 1 lettera e) del codice);
- c) **poteri di natura additiva**, che consistono nella possibilità dell'interessato di chiedere l'aggiornamento dei dati, la rettificazione ovvero, quando vi ha interesse, l'integrazione;
- d) **la facoltà di opporsi al trattamento**, per motivi legittimi, con riferimento soprattutto al trattamento svolto da pubbliche amministrazioni. -

Occorre sottolineare come questi diritti - che costituiscono diritti pieni ed esclusivi dell'interessato - possono essere esercitati in qualsiasi momento, con obbligo di risposta, salvo i casi previsti dall'articolo 8 del codice della privacy.

Il comma 4 dell'art. 8 prevede, infatti, che *“l'esercizio dei diritti considerati, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento”*.

Tale norma prevede cioè le seguenti due esclusioni dell'esercizio dei diritti dell'interessato:

- ÿ **le richieste di rettificazione o di integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o altri apprezzamenti di tipo soggettivo.** Si pensi alle diagnosi e alle valutazioni mediche di natura soggettiva, per le quali l'interessato ha un diritto pieno di conoscere i dati e le informazioni trattate, ma non può determinare, con la richiesta di rettifica o integrazioni, il giudizio del valutatore, non essendo i dati di carattere oggettivo;
- ÿ **i processi nel corso dei quali si procede all'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare.** Si pensi al fatto che nell'ambito di un ricovero ospedaliero, si ha un processo nel corso del quale dalle ipotesi iniziali, in base all'anamnesi e ai trattamenti diagnostici, si procede con una serie di attività fino alla diagnosi definitiva e all'erogazione delle prestazioni di cura e di assistenza medica e infermieristica. L'interessato può esercitare i poteri previsti dall'art. 7 del codice privacy ma, con riferimento alle diagnosi e alle decisioni e valutazioni mediche, ci possono essere momenti in cui può essere non opportuno far conoscere i dati personali oggetto di trattamento, in quanto non ancora suffragati da elementi di verosimiglianza ovvero perché si avrebbe un quadro incompleto.

L'interessato, nel caso in cui non trovi riscontro da parte del titolare o, quando designato, del responsabile, ovvero non sia soddisfatto della risposta, può far valere i diritti considerati in via alternativa presentando ricorso al Garante ovvero all'Autorità Giurisdizionale Ordinaria, la quale ha giurisdizione esclusiva, per quanto concerne ogni questione attinente al codice della privacy.

**4) l'ultimo e fondamentale adempimento riguarda l'adozione delle misure di sicurezza.** Esistono due specie di misure di sicurezza previste dal codice della privacy:

- a) le **minime**, che costituiscono la base indefettibile per la protezione dei dati personali e sono distinte a seconda della tipologia di strumenti utilizzati per il trattamento. Sono previste dagli articoli 33 e seguenti e sono specificate nell'allegato B del codice della privacy. La loro omessa adozione è sanzionata penalmente ai sensi dell'articolo 169 del codice;
- b) le **misure idonee e preventive**, che devono essere adottate, ai sensi dell'articolo 31 del codice, in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da 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 alle finalità della raccolta. La mancata adozione o la inidoneità delle misure considerate non hanno rilevanza penale, ma possono determinare una responsabilità di natura risarcitoria, ai sensi dell'articolo 15 del codice. Quest'ultimo richiama, in tema di responsabilità per i danni causati, l'articolo 2050 codice civile (riguardante le attività pericolose), per cui spetta al danneggiante dover provare di aver adottato ogni misura idonea affinché il danno non si verificasse.

## **1.7. Sanzioni previste dal codice della privacy.**

In relazione ai sopra elencati adempimenti, il codice privacy prevede nel Titolo III le diverse tipologie di sanzioni – amministrative e penali – che si riportano nella sottostante tabella:

## SANZIONI AMMINISTRATIVE

<b>Tipologia</b>	<b>Riferimento codice privacy</b>	<b>misura della sanzione</b>
Omessa o inidonea informativa	Art. 161	Dati comuni: sanzione da € 3.000 a € 18.000 Dati sensibili: sanzione da € 5.000 a € 30.000 Aumento fino al triplo in base alle condizioni economiche del contravventore
Cessione di dati	Art. 162	Sanzione da € 5.000 a € 30.000
Violazione obblighi comunicazione al paziente da parte di un medico o esercente professione sanitaria autorizzato	Art. 162, c. 2 Art. 84, c. 1	Sanzione da € 500 a € 3.000
Omessa o incompleta notificazione	Art. 163	Sanzione da € 10.000 a € 60.000
Omessa informazione o esibizione di documenti al Garante	Art. 164	Sanzione da € 4.000 a € 24.000

## SANZIONI PENALI

<b>Tipologia</b>	<b>Riferimento codice privacy</b>	<b>Sanzione prevista</b>
Trattamento illecito dei dati	Art. 167	Dati comuni: reclusione da 6 a 18 mesi Dati sensibili: reclusione da 12 a 36 mesi
Comunicazione illecita dei dati	Art. 167	Dati comuni: reclusione da 6 a 24 mesi Dati sensibili: reclusione da 1 a 3 anni
Falsità nelle dichiarazioni e notificazioni al Garante	Art. 168	Reclusione da 6 a 36 mesi
Omissione misure minime di sicurezza	Art. 169	Arresto fino a 2 anni o ammenda da € 10.000 a 50.000. Usufruendo del ravvedimento operoso e adeguandosi alle prescrizioni fissate in fase di accertamento, il reato si estingue pagando una multa di € 12.500
Inosservanza dei provvedimenti del Garante	Art. 170	Reclusione 3 - 24 mesi

In tema di responsabilità va, infine, ricordato che l'art. 15 del codice privacy prevede:  
*“Chiunque cagiona ad altri un danno per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del Codice Civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11”.*

Chiunque cagiona ad altri un danno per effetto del trattamento di dati personali è tenuto al risarcimento se non prova di avere adottato tutte le misure idonee ad evitare il danno medesimo.

Il danno non patrimoniale è risarcibile anche in caso di violazione dell'art. 11 “Modalità del trattamento e requisiti dei dati” (es. se si trattano dati non rispettandone i principi di correttezza, liceità, pertinenza ecc).

Il trattamento dei dati, quanto agli effetti della responsabilità per danno a terzi, è parificato all'esercizio di attività pericolose ex art. 2050 Codice Civile. In pratica, a fronte di danni subiti da terzi per effetto del trattamento dei dati, sarà il titolare a dover provare di aver fatto tutto quanto era possibile per evitare il danno medesimo.

## CAPITOLO 2 - Istruzioni per i responsabili e gli incaricati del trattamento

In attuazione dell'art. 29 comma 5 e dell'art. 30 comma 1, del codice privacy, si riportano di seguito le istruzioni alle quali devono attenersi i responsabili e gli incaricati nell'effettuare i trattamenti dei dati:

### 2.1. Istruzioni di carattere generale per tutti i responsabili e gli incaricati:

- ÿ **mantenere il segreto** sulle informazioni di cui si venga a conoscenza nello svolgimento della propria attività lavorativa e professionale e nel corso delle operazioni del trattamento, evitando di comunicare le informazioni a terzi. Si ricorda che l'eventuale violazione di tale obbligo può comportare l'applicazione di sanzioni di natura deontologica e disciplinare, nonché una responsabilità di natura amministrativa, civile e penale, secondo quanto previsto dal codice della privacy;
- ÿ **fornire l'informativa**, all'interessato o alla persona presso cui si raccolgono i dati, con le modalità determinate dal responsabile della struttura di appartenenza e utilizzando la modulistica predisposta dall'Azienda e allegata al presente manuale;
- ÿ **raccogliere il consenso dell'interessato** al trattamento dei dati idonei a rivelare lo stato di salute, ogniqualvolta si erogano prestazioni finalizzate alla tutela della salute (prevenzione, diagnosi, cura e riabilitazione), con le modalità e la modulistica definite dall'Azienda;
- ÿ **procedere alla raccolta dei dati personali** con la massima cura verificando l'esattezza degli stessi, nonché la pertinenza e la non eccedenza rispetto alle finalità da perseguire;
- ÿ **utilizzare** i dati solamente nei limiti del profilo di autorizzazione definito dal responsabile del trattamento e per gli scopi determinati, espressi e legittimi;
- ÿ **comunicare** i dati personali di natura comune a terzi, solamente se espressamente previsto da una legge o da un regolamento o nei casi in cui sia necessario per finalità istituzionali, previa autorizzazione dell'Azienda;
- ÿ **comunicare i dati sensibili** a soggetti determinati solo ove sia espressamente previsto da una legge o dall'atto di natura regolamentare che sarà adottato dalla Regione;
- ÿ **non diffondere dati idonei a rivelare lo stato di salute** nel rispetto dell'espresso divieto previsto dall'art. 22, comma 8 del codice privacy. Per diffusione si intende *“il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione”*. Sarà cura, quindi, dei soggetti che redigono gli atti oggetto di pubblicazione di far sì che si rispetti il divieto considerato. A titolo meramente esemplificativo, si suggerisce la necessità di predisporre la copia degli atti deliberativi da pubblicare, in una forma in cui vi sia il testo della stessa corredato da allegati (questi ultimi, contenenti i dati sanitari, non dovranno essere oggetto di pubblicazione, ma dovranno rimanere agli atti, conservati secondo quanto previsto dalla legge, e a disposizione di coloro che abbiano la legittimazione all'esercizio del diritto di accesso, secondo quanto previsto dalla legge 241/90);

### 2.2. Istruzioni specifiche per i responsabili e gli incaricati delle strutture che erogano prestazioni sanitarie (prevenzione, diagnosi, cura e riabilitazione dello stato di salute)

Il Garante per la protezione dei dati personali in data 09 novembre 2005 ha adottato, con riferimento all'art. 83 del codice privacy, un importante provvedimento con il quale ha inteso richiamare l'attenzione dei soggetti che operano in ambito sanitario – e, quindi, anche le aziende sanitarie territoriali e le aziende ospedaliere – in ordine alla necessità di adeguare il funzionamento e l'organizzazione delle strutture operative, con espresso invito ad adottare tutte le misure ritenute necessarie ed opportune per garantire il rispetto della dignità e il massimo livello di tutela dei pazienti.

In attuazione dell'art. 83 del codice privacy e dei suggerimenti del Garante, si riportano di seguito le specifiche istruzioni alle quali devono attenersi tutti i responsabili e gli incaricati delle strutture operative aziendali che erogano prestazioni sanitarie di prevenzione, diagnosi, cura e riabilitazione dello stato di salute:

#### ÿ **Dignità dell'interessato.**

La tutela della dignità personale deve essere garantita nei confronti di tutti i soggetti cui viene erogata una prestazione sanitaria con particolare riguardo a fasce deboli quali disabili, fisici e psichici, minori e anziani, nonché - per effetto di specifici obblighi di legge o di regolamento – sieropositivi o affetti da infezione da Hiv, interruzione di gravidanza e persone offese da atti di violenza sessuale.

Nei reparti di rianimazione dove si possono visitare i degenti solo attraverso vetrate o videoterminali devono essere adottati accorgimenti, anche provvisori (ad esempio mediante paraventi), che delimitino le visibilità dell'interessato durante l'orario di visita ai soli familiari e conoscenti.

I Responsabili delle strutture dove, per finalità didattiche, alcune prestazioni sanitarie vengono erogate in presenza di studenti autorizzati, oltre ad informare preventivamente ogni singolo paziente di tale modalità, devono adottare specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie.

#### ÿ **Riservatezza nei colloqui e nelle prestazioni sanitarie.**

Durante lo svolgimento di colloqui, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche), devono essere adottate idonee cautele per evitare che le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le stesse cautele devono essere adottate in occasione della raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

#### ÿ **Richiesta notizie su prestazioni di pronto soccorso.**

La notizia o la conferma di una prestazione di pronto soccorso, richieste anche per via telefonica, possono essere fornite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, valutate le diverse circostanze del caso. Il personale incaricato deve accertare l'identità dei terzi legittimati a ricevere la predetta notizia o conferma, avvalendosi anche di elementi desunti dall'interessato.

Le informazioni che possono essere fornite riguardano solo la circostanza che è in atto o si è svolta una prestazione di pronto soccorso e non anche informazioni più dettagliate sullo stato di salute dell'interessato.

L'interessato – se cosciente e capace – deve essere preventivamente informato (ad. es. in fase di accettazione) e posto in condizione di fornire indicazioni circa i soggetti che possono essere informati della prestazione di pronto soccorso. Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

#### ÿ **Dislocazione dei pazienti nei reparti.**

Il paziente cosciente e capace deve essere, all'atto del ricovero, informato e posto in condizione di fornire indicazioni circa i soggetti che possono venire a conoscenza del ricovero e del reparto di degenza. Deve essere altresì rispettata l'eventuale sua richiesta che la presenza nella struttura sanitaria non sia resa nota nemmeno ai terzi legittimati. Quando sia stato manifestato dall'interessato un consenso specifico e distinto al riguardo, possono comunque essere fornite informazioni sul suo stato di salute ai soggetti dallo stesso indicati.

#### ÿ **Distanza di cortesia.**

Nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato, tutti i punti accettazione devono essere muniti di strumenti idonei a garantire la distanza di cortesia per gli utenti. Tali strumenti possono essere costituiti, a titolo meramente esemplificativo, da una riga gialla di segnalazione posta a terra e da un cartello che indichi il rispetto della distanza di cortesia, o qualunque altro sistema, che garantisca il medesimo risultato.

#### ÿ **Ordine di precedenza e di chiamata.**

Nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa (ad es. in caso di analisi cliniche) devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli interessati che prescindano dalla loro individuazione nominativa (ad es. attribuendo loro un codice numerico o alfanumerico fornito al momento della prenotazione o dell'accettazione).

Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'interessato (ad es. nel caso di paziente disabile) possono essere utilizzati altri accorgimenti adeguati ed equivalenti come ad esempio il contatto diretto con il paziente.

Deve essere assolutamente evitata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta o di intervento effettuato o ancora da erogare (es. liste di degenti che devono subire un intervento operatorio).

#### ÿ **Correlazione fra paziente e reparto o struttura.**

Devono essere adottate specifiche procedure per prevenire che soggetti estranei possano evincere in modo esplicito l'esistenza di uno stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si è recato o è stato ricoverato.

Tali cautele devono essere adottate anche per le eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura come ad esempio le certificazioni chieste per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale.

Analoghe garanzie, infine, devono essere adottate nel caso di spedizione di plichi postali evitando che sugli stessi appaiano informazioni idonee a rivelare l'esistenza di uno stato di

salute dell'interessato come l'indicazione della tipologia del contenuto del plico o del reparto mittente.

#### ÿ **Comunicazione di dati all'interessato riguardanti il suo stato di salute.**

La comunicazione al paziente di informazioni sul suo stato di salute deve essere effettuata solo da un medico o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente stesso (ad es. un infermiere autorizzato dal Direttore di Struttura quale responsabile del trattamento dei dati).

Nel caso specifico della comunicazione all'interessato degli esiti di esami clinici effettuati, l'intermediazione può essere soddisfatta accompagnando un giudizio scritto con la disponibilità del medico a fornire ulteriori indicazioni a richiesta.

### **2.3. Istruzioni specifiche per gli incaricati addetti alla manutenzione e alla gestione degli strumenti elettronici e delle attrezzature elettromedicali.**

Agli incaricati addetti alla manutenzione e alla gestione degli strumenti elettronici e delle attrezzature elettromedicali, in servizio presso il Dipartimento Interaziendale Information Technology e la Struttura Complessa Interaziendale Ingegneria Clinica, individuati ai sensi del punto 15 del Disciplinare tecnico allegato B al codice della privacy, devono attenersi alle seguenti specifiche istruzioni:

- ÿ **verificare** in via preliminare e prima di iniziare la propria attività, l'esistenza e la disponibilità di copie di salvataggio dei dati memorizzati sugli strumenti elettronici oggetto di interventi di manutenzione;
- ÿ **verificare** la leggibilità dei dati memorizzati sui supporti contenenti le copie di salvataggio, informando gli utenti dei servizi della possibilità che alcuni dati potrebbero andare persi;
- ÿ **accedere** ai soli dati e informazioni indispensabili all'esecuzione delle azioni di assistenza e manutenzione;
- ÿ **tutelare** la riservatezza degli interessati, mantenendo il segreto su ogni notizia e informazione, acquisite in occasione dell'attività di gestione e manutenzione degli strumenti elettronici;
- ÿ **richiedere** all'operatore la parola chiave di accesso ad una applicazione solo in caso di necessità, invitando lo stesso alla modifica della sua parola chiave terminato l'intervento tecnico di assistenza;
- ÿ **custodire** i supporti rimovibili di memorizzazione ed in particolare assicurarsi sempre che non vengano dimenticati sulle postazioni (server e client) oggetto di intervento;
- ÿ **evitare** di fare o di richiedere copie di dati personali se non necessario;
- ÿ **cancellare** le copie di dati personali, su supporti rimovibili, che non siano più necessarie per finalità di manutenzione e assistenza tecnica;
- ÿ **provvedere** alla distruzione dei dischi non riscrivibili che contengano dati personali sensibili o giudiziari che non sia necessario detenere o utilizzare;
- ÿ **prelevare** dalle apparecchiature informatiche o elettromedicali da dismettere tutti i supporti di memoria provvedendo, se autorizzato, alla loro distruzione controllata.

## **2.4. Istruzioni specifiche per tutti i responsabili e gli incaricati per il corretto uso e la sicurezza degli strumenti aziendali e la protezione dei dati personali.**

### **1 - Utilizzo del personal computer in dotazione**

- 1) utilizzare il personal computer in dotazione, esclusivamente per ragioni di lavoro e per conto dell'azienda;
- 2) assicurarsi che quando si sta lavorando al computer nessuno possa conoscere i dati che si stanno digitando o i file su cui si sta lavorando, ponendo attenzione a posizionare il monitor in modo da evitare che persone estranee possano visualizzare la schermata di lavoro;
- 3) disconnettere la sessione di lavoro ogni qual volta si abbandona, anche momentaneamente, la propria postazione;
- 4) in alternativa al punto 3), utilizzare lo screen-saver protetto con password in modo da evitare che in caso di prolungata assenza i dati possano essere accessibili a soggetti estranei;
- 5) spegnere il computer in caso di assenza prolungata dal posto di lavoro. Un computer acceso è maggiormente attaccabile in quanto raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Lasciare un computer acceso aumenta il rischio che un'interruzione dell'energia elettrica possa causare un danno;
- 7) non lasciare mai incustodito un notebook aziendale in ufficio o in viaggio (particolare attenzione deve essere riposta quando si viaggia sui mezzi pubblici);
- 8) durante le missioni di lavoro, portare il notebook come bagaglio a mano, evitando di trasportare in borsa i codici identificativi e le parole chiave di sicurezza, nonché i supporti di memorizzazione con le copie di back-up;
- 9) non lasciare esposto in automobile in sosta il notebook aziendale.

### **2 - Password**

- 1) la password, assegnata a ciascun responsabile e incaricato, deve essere prontamente sostituita al primo utilizzo e deve essere modificata con cadenza almeno trimestrale;
- 2) la password non deve contenere riferimenti agevolmente riconducibili al titolare della stessa e deve essere generata preferibilmente senza un significato compiuto;
- 3) nello scegliere la propria password, devono essere utilizzati anche caratteri speciali e lettere maiuscole e minuscole;
- 4) la password deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- 5) il titolare della password è responsabile di ogni utilizzo indebito o non consentito della stessa;
- 6) fare attenzione a non essere "spiati" durante la digitazione di una password o qualunque codice di accesso;
- 7) non permettere l'uso della propria password da parte di soggetti terzi, per cui solamente in caso di necessità richiedere la finalità della richiesta (intervento di assistenza o di manutenzione) e accertarsi dell'identità del soggetto che richiede la comunicazione della vostra password.

### **3 - Dati**

- 1) I dati devono essere trattati con liceità e correttezza;
- 2) il trattamento dei dati è ammesso solamente per uno scopo determinato, esplicito e legittimo;
- 3) i dati oggetto di trattamento devono essere pertinenti, non eccedenti e completi rispetto alle finalità perseguite;
- 4) nel caso di trattamento di dati sensibili o giudiziari devono essere trattati i dati indispensabili per gli scopi del proprio agire.

#### **4 – Supporti di memorizzazione**

- 1) se possibile, salvare sempre le informazioni confidenziali sul vostro server di rete e non sull'hard disk del personal computer in dotazione;
- 2) non salvare informazioni di natura sensibile su floppy-disk;
- 3) le pen drive in cui sono memorizzati i dati personali devono essere conservate e non cedute a terzi;
- 4) nel caso di utilizzo di pen drive, per la memorizzazione di dati, fare attenzione a disinserire le chiavi dalle porte USB seguendo la procedura di disconnessione sicura;
- 5) nel caso in cui le pen drive sono consegnate a terzi per trasferire dati, assicurarsi che sulla chiave di memorizzazione siano presenti solamente i dati necessari da trasferire, ovvero effettuare personalmente l'operazione di trasferimento, evitando di consegnare la chiave a terzi, che potrebbero copiare le informazioni personali memorizzate;
- 6) eliminare documenti, dischetti o altri supporti di memorizzazione in maniera sicura, evitando di gettarli nel cestino della spazzatura, senza averli previamente resi inutilizzabili;
- 7) accertarsi che le informazioni non più utili vengano cancellate in modo sicuro dai supporti di dati e non conservare inutilmente messaggi di posta elettronica.

#### **5 - Virus**

- 1) i virus possono alterare o addirittura distruggere i dati e i programmi;
- 2) i virus diffusi in internet sono spesso camuffati da programmi di utilità o di intrattenimento;
- 3) ogni computer deve essere protetto da idonei strumenti per il rischio di attività di virus informatici;
- 4) lo strumento di protezione (di norma software antivirus) deve essere abilitato;
- 5) è vietato disattivare, senza autorizzazione del Dipartimento Interaziendale Information Technology, il software antivirus;
- 6) la posta elettronica viene filtrata in entrata da un apposito prodotto antivirus che pulisce gli eventuali allegati contenenti virus. Evitare di aprire messaggi provenienti da mittenti sconosciuti o sospetti e cancellarli immediatamente;
- 7) nel caso di utilizzo di supporti di memorizzazione esterni, controllare sempre che i file memorizzati non siano infettati da virus attraverso la scansione del supporto;
- 8) controllare periodicamente la presenza di virus sul proprio computer in dotazione mediante la scansione dell'intero sistema.

#### **6 - Software**

- 1) sul computer in dotazione può essere utilizzato solamente il software fornito dall'azienda;
- 2) non si possono installare software e applicazioni senza una specifica autorizzazione da parte del Dipartimento Interaziendale Information Technology (DIIT);
- 3) non installare da soli i software sul personal computer in dotazione, se non previa autorizzazione da parte del Dipartimento Interaziendale Information Technology;
- 4) non creare e non utilizzare software senza licenza d'uso.

## **7 – Posta elettronica**

- 1) Ogni utente deve utilizzare la posta elettronica messa a disposizione dall'azienda (con indirizzo dell'ente) esclusivamente per necessità di lavoro;
- 2) i messaggi di posta elettronica ricevuti o spediti con l'indirizzo di posta elettronica aziendale non costituiscono corrispondenza personale del dipendente o collaboratore aziendali, per cui possono essere conosciuti da terzi per esigenze operative e istituzionali;
- 3) le informazioni trasmesse – molto spesso - possono / devono essere condivise per cui deve essere salvaguardata l'integrità e la confidenzialità dei messaggi e dei contenuti;
- 4) si deve evitare di rispondere alle cd. catene di Sant'Antonio degli utenti di internet o ai messaggi di solidarietà che richiedono di inviare un'e-mail a un certo indirizzo o a un certo numero di utenti, poiché possono essere veicoli di diffusione di virus informatici ovvero sistemi per la raccolta di indirizzi di posta elettronica, per l'invio di comunicazioni commerciali non desiderate o di posta cd. spazzatura;
- 5) evitare di rispondere a messaggi promozionali o di spamming;
- 6) evitare di trasmettere per posta elettronica contenuti che possano essere considerati di contenuto molesto/osceno, razzista, pedo-pornografico o illegale, nonché aventi natura ingiuriosa o diffamatoria;
- 7) evitare di registrare il proprio indirizzo di posta elettronica su siti web sospetti e/o mailing list non direttamente correlate all'attività istituzionale aziendale;

## **8 - Internet**

- 1) Internet deve essere utilizzato esclusivamente per ragioni di lavoro;
- 2) non si deve utilizzare l'accesso ad internet per fini personali, che esulano dall'attività lavorativa;
- 3) è vietato accedere a siti web contenenti materiale pedo-pornografico, materiale fraudolento-illegale, materiale blasfemo/molesto/osceno;
- 4) è, altresì, vietato tentare di violare o aggirare i sistemi di controllo o di protezione dell'uso di internet e della posta elettronica installati e utilizzati dall'azienda, nel rispetto del diritto alla riservatezza dei dipendenti;
- 5) è, infine, vietato installare e/o utilizzare in modo fraudolento strumenti concepiti per compromettere la sicurezza dei sistemi (ad esempio strumenti di "password cracking", "network probing",...).

## **9 – Rete di comunicazione**

- 1) è vietato allacciare alla rete di comunicazione aziendale strumenti elettronici che non siano stati forniti dall'Azienda;
- 2) il computer in dotazione non deve possedere o disporre di altri collegamenti esterni diretti;
- 3) è vietato installare mezzi di comunicazione propri (come per esempio il modem analogico);
- 4) utilizzare esclusivamente le installazioni messe a disposizione dall'azienda ovvero quelle che siano oggetto di specifica autorizzazione;
- 5) non usare mai il proprio user-id e la propria password per accedere a sistemi esterni;
- 6) ricorrere, eventualmente, a sistemi esterni solamente per finalità istituzionali e di lavoro;
- 7) ricordarsi che l'azienda può monitorare il lavoro svolto e le connessioni, potendo verificare quali siti siano stati visitati e quali operazioni di trattamento sono svolte con i dati personali, di cui è titolare l'azienda;
- 8) non inviare informazioni confidenziali tramite internet o altre reti di comunicazione elettronica senza aver preso le dovute precauzioni e adottato le misure di sicurezza idonee a ridurre i rischi di accesso abusivo dei dati trasmessi.

## **10 – Utilizzo di telefono e fax**

- 1) In generale, è opportuno non fornire indicazioni relative allo stato di salute degli utenti via telefono, se non si è certi dell'identità dell'interlocutore che sta chiamando;
- 2) verificare comunque che l'interessato abbia autorizzato la comunicazione dei propri dati a terzi;
- 3) in alcuni casi, specie per chiamate di natura istituzionale (da altre strutture ospedaliere, autorità giudiziaria, soggetti pubblici), si consiglia di farsi lasciare dal chiamante il proprio nominativo e il numero di telefono; si provvederà a ricontattare l'ente chiamante, chiedendo della persona che ha lasciato il proprio nominativo, previa verifica dell'indispensabilità dei dati richiesti rispetto alla finalità dell'utilizzo dichiarato e della previsione normativa o dell'autorizzazione dell'interessato alla comunicazione dei propri dati;
- 4) nel caso in cui si debba procedere alla comunicazione di dati sensibili tra unità diverse utilizzando il fax, è opportuno che lo strumento sia collocato in un'area protetta e presidiata e che i responsabili e gli incaricati prestino attenzione alle fasi di invio (verifica della corretta digitazione del numero del destinatario, inserimento di formula di riservatezza) e di ricevimento della documentazione contenente dati personali sensibili;
- 5) nel caso in cui si debbano comunicare ad un ente o soggetto esterni dati sensibili utilizzando il fax, in occasione del primo rapporto con l'ente, si deve richiedere, prima dell'invio della documentazione, di indicare il numero di un fax, localizzato in luogo protetto e non accessibile al pubblico, al quale inviare la documentazione;
- 6) il riscontro alla richiesta di cui al punto precedente, avrà come effetto l'autorizzazione all'azienda ad inviare esclusivamente al numero dichiarato la documentazione considerata. Ogni operatore incaricato del trattamento deve conservare copia della comunicazione di elezione del numero di fax, indicato per la ricezione di fax riservati.

## **11 – Utilizzo della stampante**

- 1) la stampa di documentazione contenente dati personali e sensibili deve avvenire ad opere di incaricati autorizzati a trattare tali dati;
- 2) ritirare tempestivamente la documentazione dalla stampante utilizzata;
- 3) il riutilizzo di fogli recanti una stampa su una sola facciata, per esigenze di risparmio e di sensibilità ambientale, deve riguardare esclusivamente supporti nella esclusiva disponibilità dell'incaricato ed essere utilizzati nell'ambito delle proprie mansioni, evitando di far conoscere a terzi non autorizzati il contenuto dei documenti;
- 4) i fogli contenenti dati personali e sensibili non più utilizzati e per i quali non è necessaria la conservazione, prima di essere conferiti nella raccolta differenziata, devono essere trattati in modo da rendere non intelligibili a terzi – usando eventualmente un dispositivo distruggi documenti – dati personali ivi contenuti.

## **12 – Utilizzo della fotocopiatrice**

- 1) la foto riproduzione di documentazione cartacea, contenente dati personali e, in particolare, dati, sensibili deve avvenire ad opera dell'incaricato autorizzato a trattare tali dati

### **2.5. Istruzioni per i responsabili e gli incaricati per il corretto trattamento dei dati su supporto cartaceo.**

- ÿ quando le cartelle cliniche o altra documentazione contenente dati idonei a rivelare lo stato di salute devono essere trasferite da una struttura o da un ufficio presso altro luogo (esempio archivio di deposito) è necessario utilizzare cautele per la protezione della riservatezza al fine di impedire un accesso non autorizzato a tale documentazione. Si consiglia di inserire la documentazione in busta chiusa o in raccoglitori sigillati sui quali apporre la propria firma per garantirne l'integrità;
- ÿ i locali adibiti ad archivio all'interno di ciascuna struttura, in cui siano conservati documenti contenenti dati personali di natura sensibile, devono essere chiusi a chiave e le chiavi devono essere custodite da personale autorizzato (accesso selezionato);
- ÿ evitare di scrivere dati personali di natura sensibile su lavagne o altri supporti che possano essere visionati da persone non autorizzate;
- ÿ le cartelle e i fascicoli di lavoro devono essere tenuti sulla propria scrivania facendo attenzione che i dati eventualmente riportati sul frontespizio non siano visibili a persone non autorizzate (es. utenti del servizio);
- ÿ nel caso di assenza, anche momentanea, dalla propria stanza, non lasciare incustoditi fascicoli, cartelle e documenti cartacei contenenti dati di natura sensibile. Si consiglia di chiudere a chiave la propria stanza, qualora rimanga incustodita senza personale all'interno, ovvero di riporre la documentazione dentro un armadio chiuso a chiave.