VADEMECUM
per uso didattico e formativo

a cura di Fabio Trojani

avvocato specialista in diritto amministrativo
esperto in diritto della protezione dei dati personali

INDICE

Capitolo 01
Elementi introduttivi sul d. lgs. 196/2003 (codice della privacy)

Capitolo 02
Protezione dei dati e rispetto della dignità degli assistiti

Capitolo 03
Decalogo per la sicurezza degli strumenti e per la protezione dei dati personali

CAPITOLO 01
Elementi introduttivi sul d. lgs. 196/2003 (codice della privacy)

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 (o l'azienda ospedaliera) 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, se ciò è affermativo, in quale contesto e con quali forme.

Accanto al diritto alla riservatezza, anche a causa del progresso tecnologico, il concetto di privacy si è evoluto da "diritto ad essere lasciato solo" a diritto 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 dati personali, che si sostanzia da un lato nella facoltà per ciascun interessato di poter esercitare i diritti previsti dall'art. 7 del codice della privacy e dall'altro nell'obbligo per il titolare del trattamento di adottare misure di sicurezza a protezione dei dati personali e nel dover rispondere all'interessato, che eserciti i diritti previsti dal citato art. 7.

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 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 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) da quelle 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 anche l'aggiornamento, se necessario, 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.

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:

a) 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 ala 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 erp i tossicodipendenti (DPR 309/1990). 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 alla natura soggettiva del 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. 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 ampie e onnicomprensive come "dati idonei a rivelare …". 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,…;

b) 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;

c) 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;

d) 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.

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), obbligo che si ricollega direttamente anche all'informazione prevista in tema di avvio del procedimento amministrativo (cfr. articolo 7 legge 241/90);
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 dette 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 dei dati, 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.

5. I profili soggettivi del rapporto di 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.

Nel caso in cui si proceda al trattamento di dati aggregati e anonimi, ovvero cifrati, senza che il titolare abbia la possibilità di risalire alla identificazione del soggetto, la normativa in materia di tutela della privacy non troverà applicazione per ovvi motivi, in quanto non sarà determinabile l'identità di alcun soggetto.

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 è titolare del trattamento come entità**, non essendo corretto qualificare il Direttore Generale come titolare del trattamento.

Il DG rappresenta l'ente, che è il titolare come entità in sé.
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.

In secondo luogo, nelle organizzazione complesse, come può essere quella di un'azienda sanitaria o ospedaliera, vi è la necessità di provvedere alla nomina di uno o più **responsabili del trattamento**, che, ai sensi dell'articolo 4, comma 1 lettera g) del codice, è definito come "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali".

L'articolo 29 dispone che ove designato il responsabile "è individuato 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"; si aggiunge, inoltre, che "ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti", i quali devono essere "analiticamente specificati per iscritto dal titolare".

Per procedere alla nomina occorre la necessaria formalizzazione dei compiti attribuiti ai responsabili, i quali dovranno ricevere, altresì, istruzioni scritte riferite allo svolgimento dei compiti medesimi affidati loro.

Il DG, in qualità di rappresentante legale dell'azienda, con la delibera di approvazione del presente vademecum ha altresì nominato i responsabili del trattamento nelle persone dei responsabili pro-tempore delle strutture operative complesse aziendali ovvero nei Direttori di Dipartimento, che non siano ripartiti in strutture complesse, o, infine, nei responsabili pro-tempore delle strutture operative semplici, che non facciano parte di strutture complesse.

Nella struttura piramidale che caratterizza l'organizzazione da designare per il trattamento dei dati, alla base troviamo gli **incaricati del trattamento**, che sono definiti dal codice come le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Vi è, di conseguenza, l'obbligo di procedere alla individuazione in qualità di incaricati di tutti coloro che a vario titolo sono preposti allo svolgimento delle operazioni di trattamento per conto dell'azienda, i quali hanno necessità di accedere ai dati personali e che operano sotto la diretta autorità dell'ente titolare o dei oggetti nominati responsabili.

L'individuazione di una persona come incaricato determina, come conseguenza, il venir meno della posizione di terzietà del soggetto considerato, che al fine dello svolgimento delle operazioni di trattamento deve poter conoscere i dati, con la conseguenza che la necessaria formalizzazione della sua preposizione unitamente alla esplicazione di istruzioni scritte impartite fa venir meno la qualificazione della conoscenza dei dati come operazione di comunicazione, secondo quanto detto in precedenza.

In conclusione, ciascuna persona chiamata allo svolgimento di operazioni di trattamento è incaricata del trattamento con specifico riferimento al ruolo professionale e alla categoria di appartenenza e alla struttura in cui è formalmente preposta, per la quale risulti determinato in modo analitico l'ambito di trattamento consentito agli operatori, che svolgono compiti e mansioni in seno alla stessa, sotto la diretta autorità del titolare o del responsabile.

6. Linee guida sui singoli adempimenti previsti dal codice per i soggetti pubblici

1) L'**informativa**: costituisce un obbligo ascritto alla trasparenza dei trattamenti ed è prevista dall'articolo 13 del codice:

a) deve 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 svolto 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 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) l'informativa deve contenere gli elementi elencati dall'articolo 13 del codice; di contro, è espressamente previsto che ove l'interessato sia a conoscenza di alcuni elementi questi possono essere omessi;
e) l'informativa può essere fornita anche in forma orale; tuttavia, a seconda delle modalità di raccolta del dato e del rapporto con gli interessati, si consiglia di fornire l'informativa attraverso manifesti (nel caso di rapporti di sportello), 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 domande, di

istanze procedimentali o per la richiesta di prestazioni o servizi. Appare opportuno pubblicare le diverse formule di informativa sul sito internet dell'ente;

f) l'informativa può essere fornita anche dall'incaricato del trattamento;
g) l'omessa informativa o la sua inidoneità sono condotte sanzionate ai sensi dell'articolo 161 del codice della privacy

2) **legittimazione al trattamento:** per poter trattare i dati personali i soggetti pubblici non devono richiedere il consenso degli interessati (salvo quanto previsto dagli articoli 76 e 110 del codice della privacy, che riguardano il trattamento dei dati idonei a rivelare lo stato di salute da parte di organismi sanitari pubblici per finalità, rispettivamente, di tutela della salute o dell'incolumità fisica dell'interessato ovvero per scopi di ricerca scientifica, in campo medico, biomedico o epidemiologico).

I soggetti pubblici sono legittimati al trattamento in base al principio di finalità istituzionale.

In particolare, nel caso del **trattamento avente ad oggetto i dati comuni** (cfr. articoli 18 e 19 del codice) occorrerà distinguere tra l'esercizio delle operazioni di processo interno e le ipotesi di comunicazione e di diffusione dei dati ivi considerati:

a) per raccogliere e trattare i dati comuni è sufficiente che il trattamento sia strumentale all'esercizio di finalità istituzionali dell'azienda;
b) per la **comunicazione** di dati comuni **a soggetti privati** occorre sempre e necessariamente una **previsione di legge o di regolamento**;
c) per poter **comunicare dati comuni a soggetti pubblici** occorre, come nel caso precedente, una espressa previsione di **legge** o di **regolamento,** ovvero, in mancanza di una previsione normativa, ma ove l'operazione considerata (ossia la comunicazione di dati diversi da quelli sensibili o giudiziari dall'azienda ad altro soggetto pubblico, ad esempio ad un Comune o alla Regione) sia **necessaria per l'esercizio di funzioni istituzionali** occorrerà fornire comunicazione preliminare di tale circostanza al Garante per la protezione dei dati personali (ai sensi dell'articolo 39, comma 1 del codice) ed attendere quarantacinque giorni.

Per poter trattare i **dati sensibili** occorre, invece, una **espressa previsione di legge** (ai sensi dell'articolo 20, comma 1 del codice), che autorizzi il trattamento considerato, prevedendo le rilevanti finalità di interesse pubblico, i tipi di dati e le operazioni eseguibili.

Tuttavia, ove la legge individui le rilevanti finalità di interesse pubblico (autorizzando così il trattamento dei dati sensibili), ma non la specifica determinazione dei tipi di dati e delle operazioni, secondo quanto detto, occorrerà adottare un regolamento ai sensi dell'articolo 20, comma 2.

L'azienda, non essendo dotata di potestà regolamentare ad efficacia esterna, non può adottare atti che determinino i tipi di dati sensibili e le operazioni che possono essere eseguite; tale adempimento è ascritto alla Regione, che, in qualità di titolare del servizio sanitario, ha la potestà di regolare e organizzare il servizio, con specifica competenza ad adottare norme di regolamento per la disciplina del trattamento dei dati ivi considerati, previo parere obbligatorio e vincolante del Garante per la protezione dei dati personali.

Il regolamento deve essere adottato dalla Regione Veneto entro il 15 maggio 2006 (termine così da ultimo prorogato).

3) **la notificazione al Garante:** doveva essere effettuata entro il **30 aprile 2004** (da parte dell'azienda) secondo quanto previsto dall'articolo 37 del codice della privacy.

4) gestione delle istanze presentate dall'interessato, aventi ad oggetto **l'esercizio dei diritti di cui all'articolo 7 del codice**, che possono riguardare tre ordine di categorie:

a) **diritto di accesso:** consiste nella facoltà di ottenere la conferma dell'esistenza o meno di dati personali che riguardano l'interessato e la loro comunicazione in forma intelligibile. Inoltre, l'interessato può ottenere 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) **diritti di natura inibitoria:** concernono la possibilità 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). Rientra in tale categoria di diritti anche la facoltà di opposizione al trattamento per motivi legittimi, ancorché i dati siano pertinenti allo scopo della raccolta. La differenza tra quest'ultima facoltà e quelle considerate in precedenza sta nel fatto che la cancellazione, il blocco o la trasformazione in forma anonima presuppongono la violazione di legge, al contrario dell'opposizione (che deve essere suffragata da motivi legittimi), con ciò fungendo

da contrappeso alla circostanza per cui i soggetti pubblici trattano i dati personali senza dover richiedere il consenso dell'interessato, il quale potrà tutelarsi da questa ingerenza nella sua sfera di riservatezza adducendo le motivazione legittime a seconda dei casi concreti considerati;

c) infine, **diritti di natura additiva**, che sono direttamente connessi al generale principio di garanzia di qualità dei dati (secondo quanto previsto dall'articolo 11, comma 1 lettera c) del codice): l'interessato può, infatti, richiedere l'aggiornamento dei dati, la rettificazione ovvero, quando vi ha interesse, l'integrazione.

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

Va infine considerato quanto previsto dall'articolo 8, comma 4, secondo cui "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".

L'interessato, nel caso in cui non trovi riscontro da parte del titolare, ovvero non sia soddisfatto di ciò, 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.

Occorre peraltro considerare l'art. 84, comma 1 del codice della privacy, che impone che "i dati idonei a rivelare lo stato di salute possono essere fatti conoscere all'interessato o - nel caso di incapacità di agire o di incapacità di intendere o di volere di quest'ultimo – "all'esercente la potestà ovvero ai familiari, prossimi congiunti o conviventi, oppure, in mancanza, al responsabile della struttura presso cui dimori" solo per il tramite di un medico designato dall'interessato o dal titolare.
La disposizione ha il fine di tutelare l'integrità psico-fisica dell'interessato rispetto alla conoscenza di dati personali idonei a rivelare lo stato di salute di natura particolare, che possono determinare disagi psicologici, contraccolpi sull'equilibrio emotivo. Si prevede, di conseguenza, l'obbligo della necessaria mediazione medica, ossia del professionista ritenuto più idoneo per conoscenze, professionalità e preparazione a conferire con il paziente.

Peraltro, il comma 2 del medesimo articolo dispone che il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali di salute, a rendere noti i medesimi dati all'interessato o ai soggetti considerati, nel caso di incapacità o impossibilità fisica di quest'ultimo;

5) **l'adozione di misure di sicurezza:** esistono due specie di misure di sicurezza previste dal codice della privacy:

a) quelle **minime** (riportate nella tabella in calce): 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 (si ha quella che viene definita un'inversione dell'onere della prova, secondo alcuni, ovvero una responsabilità per colpa lievissima, secondo altri).

CAPITOLO 02
Protezione dei dati e rispetto della dignità degli assistiti

1. Prescrizioni del Garante – provvedimento del 09 novembre 2005

Strutture sanitarie: rispetto della dignità

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali (direttiva n. 95/46/CE), anche in relazione agli articoli 2, 10, 11 e 32 della Costituzione;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

CONSIDERATO:

1. Premessa

Sono pervenuti a questa Autorità reclami e segnalazioni con i quali si rappresenta che alcune strutture sanitarie, nell'erogare prestazioni e servizi per finalità di prevenzione, diagnosi, cura e riabilitazione, non rispetterebbero le garanzie previste dalla legge a tutela, in particolare, della dignità e della riservatezza delle persone interessate.

In materia di trattamento dei dati personali in ambito sanitario, il Codice prevede che gli organismi sanitari pubblici e privati adottino misure ed accorgimenti di carattere supplementare rispetto a quelle già previste per il trattamento dei dati sensibili e per il rispetto delle misure di sicurezza. In particolare, l'art. 83 individua alcune specifiche prescrizioni che devono tradursi anche in adeguate misure organizzative, ferma restando la necessità di adottare comunque tutti gli ulteriori accorgimenti che si rendessero opportuni per garantire il più ampio rispetto dei diritti e delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale.

Con il presente provvedimento, il Garante intende richiamare l'attenzione dei soggetti che operano in ambito sanitario in ordine alla necessità di adeguare il funzionamento e l'organizzazione delle strutture sanitarie alle previsioni stabilite dal Codice in materia di protezione di dati personali (art. 83). I medesimi soggetti sono altresì invitati ad adottare tutte le misure ritenute necessarie ed opportune, conformemente ai principi generali, per garantire il rispetto della dignità della persona e il massimo livello di tutela degli interessati in ambito sanitario.

2. Ambito di applicazione delle misure per il rispetto dei diritti degli interessati

Le misure organizzative in esame devono essere adottate per espresso obbligo di legge da tutti gli organismi sanitari, sia pubblici (es. aziende sanitarie territoriali, aziende ospedaliere), sia privati (es. case di cura).

Sono tenuti alla loro adozione anche i servizi e le strutture di soggetti pubblici operanti in ambito sanitario o aventi competenza in materia di prevenzione e sicurezza del lavoro (es. osservatori epidemiologici regionali, servizi di prevenzione e sicurezza sul lavoro).

I medici di medicina generale e i pediatri di libera scelta, nonché, deve ritenersi, anche i medici specialisti operanti in studi medici privati, non sono invece destinatari dell'obbligo di adottare dette misure, che riguardano l'organizzazione di strutture. I medesimi soggetti devono comunque ottemperare ai principi cui si ispirano le disposizioni in esame, predisponendo in ogni caso misure idonee a garantire il rispetto dei diritti e delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, secondo modalità adeguate a garantire un rapporto personale e fiduciario con gli assistiti (art. 83, comma 2-bis, del Codice).

3. Garanzie per l'interessato

Gli organismi sanitari pubblici e privati, in qualità di titolari del trattamento dei dati personali, devono garantire, in particolare, il rispetto dei seguenti princìpi:

a) dignità dell'interessato (art. 83, comma 2, lett. e) del Codice)

La prestazione medica e ogni operazione di trattamento dei dati personali deve avvenire nel pieno rispetto della dignità dell'interessato (artt. 2 e 83 del Codice).

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 i disabili, fisici e psichici, i minori, gli anziani e i soggetti che versano in condizioni di disagio o bisogno.

Particolare riguardo deve essere prestato nel rispettare la dignità di pazienti sottoposti a trattamenti medici invasivi o nei cui confronti è comunque doverosa una particolare attenzione anche per effetto di specifici obblighi di legge o di regolamento o della normativa comunitaria (ad es., in riferimento a sieropositivi o affetti da infezione da Hiv —l. 5 giugno 1990, n. 135-, all'interruzione di gravidanza —l. 22 maggio 1978, n. 194- o a persone offese da atti di violenza sessuale -art. 734-bis del codice penale-).

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

La necessità di rispettare la dignità è stata rappresentata a questa Autorità anche in relazione alle modalità di visita e di intervento sanitario effettuati nelle aziende ospedaliero-universitarie alla presenza di studenti autorizzati. Le strutture che intendono avvalersi di questa modalità devono indicare nell'informativa da fornire al paziente che (art. 13 del Codice), in occasione di alcune prestazioni sanitarie, si perseguono anche finalità didattiche, oltre che di cura e prevenzione (cfr. d.lg. n. 517/1999). Durante tali prestazioni devono

essere adottate 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.

b) riservatezza nei colloqui e nelle prestazioni sanitarie (art. 83, comma 2, lett. c) e d))

É doveroso adottare idonee cautele in relazione allo svolgimento di colloqui, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

Il rispetto di questa garanzia non ostacola la possibilità di utilizzare determinate aree per più prestazioni contemporanee, quando tale modalità risponde all'esigenza terapeutica di diminuire l'impatto psicologico dell'intervento medico (ad es., alcuni trattamenti sanitari effettuati nei confronti di minori).

c) notizie su prestazioni di pronto soccorso (art. 83, comma 2, lett. f))

L'organismo sanitario può dare notizia, anche per via telefonica, circa una prestazione di pronto soccorso, ovvero darne conferma a seguito di richiesta anche per via telefonica.

La notizia o la conferma devono essere però fornite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, valutate le diverse circostanze del caso.

Questo genere di informazioni riguarda solo la circostanza che è in atto o si è svolta una prestazione di pronto soccorso, e non attiene ad informazioni più dettagliate sullo stato di salute.

L'interessato -se cosciente e capace- deve essere preventivamente informato dall'organismo sanitario (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.

Il personale incaricato deve accertare l'identità dei terzi legittimati a ricevere la predetta notizia o conferma, avvalendosi anche di elementi desunti dall'interessato.

d) dislocazione dei pazienti nei reparti (art. 83, comma 2, lett. g))

Il Codice incentiva le strutture sanitarie a prevedere, in conformità agli ordinamenti interni, le modalità per fornire informazioni ai terzi legittimati circa la dislocazione dei degenti nei reparti, allorché si debba ad esempio rispondere a richieste di familiari e parenti, conoscenti e personale del volontariato.

L'interessato cosciente e capace deve essere, anche in questo caso, informato e posto in condizione (ad es. all'atto del ricovero) di fornire indicazioni circa i soggetti che possono venire a conoscenza del ricovero e del reparto di degenza. Occorre altresì rispettare l'eventuale sua richiesta che la presenza nella struttura sanitaria non sia resa nota neanche ai terzi legittimati (cfr. Carta dei servizi pubblici sanitari, dPCM 19 maggio 1995).

Come per le prestazioni di pronto soccorso, questo genere di informazioni riguarda la sola presenza nel reparto e non anche informazioni sullo stato di salute.

Possono essere fornite informazioni sullo stato di salute a soggetti diversi dall'interessato quando sia stato manifestato un consenso specifico e distinto al riguardo, consenso che può essere anche manifestato da parte di un altro soggetto legittimato, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato (art. 82).

e) distanza di cortesia (art. 83, comma 2, lett. b))

Le strutture sanitarie devono predisporre apposite distanze di cortesia in tutti i casi in cui si effettua il trattamento di dati sanitari (es. operazioni di sportello, acquisizione di informazioni sullo stato di salute), nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato.

Vanno in questa prospettiva prefigurate appropriate soluzioni, sensibilizzando gli utenti con idonei inviti, segnali o cartelli.

f) ordine di precedenza e di chiamata (art. 83, comma 2, lett. a))

All'interno dei locali di strutture sanitarie, 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 prescinda dalla loro individuazione nominativa (ad es., attribuendo loro un codice numerico o alfanumerico fornito al momento della prenotazione o dell'accettazione). Ovviamente, tale misura non deve essere applicata durante i colloqui tra l'interessato e il personale medico o amministrativo.

Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'interessato (ad es. in funzione di particolari caratteristiche del paziente anche legate ad uno stato di disabilità), possono essere utilizzati altri accorgimenti adeguati ed equivalenti (ad es., con un contatto diretto con il paziente).

Non risulta giustificata 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). Non devono essere, parimenti, resi facilmente visibili da terzi non legittimati i documenti riepilogativi di condizioni cliniche dell'interessato (es. cartelle infermieristiche poste in prossimità del letto di degenza) (artt. 22, comma 8, e 26, comma 5, del Codice).

g) correlazione fra paziente e reparto o struttura (art. 83, comma 2, lett. h))

Gli organismi sanitari devono mettere in atto specifiche procedure, anche di formazione del personale, 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 orientate anche alle eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura (ad es., per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale).

Analoghe garanzie devono essere adottate da tutti i titolari del trattamento, ivi comprese le farmacie, affinché nella spedizione di prodotti non siano indicati, sulla parte esterna del plico postale, informazioni idonee a rivelare l'esistenza di uno stato di salute dell'interessato (ad es., indicazione della tipologia del contenuto del plico o del reparto dell'organismo sanitario mittente).

h) regole di condotta per gli incaricati (art. 83, comma 2, lett. i)).

Il titolare del trattamento deve designare quali incaricati o, eventualmente, responsabili del trattamento i soggetti che possono accedere ai dati personali trattati nell'erogazione delle prestazioni e dei servizi per svolgere le attività di prevenzione, diagnosi, cura e riabilitazione, nonché quelle amministrative correlate (artt. 30 e 29 del Codice).

Fermi restando, in quanto applicabili, gli obblighi in materia di segreto d'ufficio, deve essere previsto che, al pari del personale medico ed infermieristico, già tenuto al segreto professionale (art. 9 del codice di deontologia medica del 3 ottobre 1998; art. 4 del codice deontologico per gli infermieri del maggio del 1999), gli altri soggetti che non sono tenuti per legge al segreto professionale (ad es., personale tecnico e ausiliario) siano sottoposti a regole di condotta analoghe (cfr. anche art. 10 del codice di deontologia medica).

A tal fine, anche avvalendosi di iniziative di formazione del personale designato, occorre mettere in luce gli obblighi previsti dalla disciplina in materia di protezione dei dati personali con particolare riferimento all'adozione delle predette misure organizzative (artt. 30 e 35 del Codice e punto 19.6 del disciplinare tecnico allegato B) al Codice), evidenziando i rischi, soprattutto di accesso non autorizzato, che incombono sui dati idonei a rivelare lo stato di salute e le misure disponibili per prevenire effetti dannosi.

4. Comunicazione di dati all'interessato

Gli esercenti le professioni sanitarie e gli organismi sanitari possono comunicare all'interessato informazioni sul suo stato di salute solo per il tramite di un medico (individuato dallo stesso interessato, oppure dal titolare del trattamento) o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente (ad es., un infermiere designato quale incaricato del trattamento ed autorizzato per iscritto dal titolare).

La necessità di rispettare queste modalità andrebbe menzionata nelle istruzioni impartite agli incaricati del trattamento (art. 84, comma 2, del Codice). Nel caso in cui l'interessato riceva una comunicazione dalla struttura sanitaria che documenti gli 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.

Il personale designato deve essere istruito debitamente anche in ordine alle modalità di consegna a terzi dei documenti contenenti dati idonei a rivelare lo stato di salute dell'interessato (es. referti diagnostici). In riferimento alle numerose segnalazioni pervenute, va rilevato che le certificazioni rilasciate dai laboratori di analisi o dagli altri organismi sanitari possono essere ritirate anche da persone diverse dai diretti interessati, purché sulla base di una delega scritta e mediante la consegna delle stesse in busta chiusa.

5. Altri adempimenti da rispettare

I titolari del trattamento in ambito sanitario devono infine rispettare gli obblighi che attengono:

a) alla notificazione al Garante, dovuta nei soli casi di cui all'art. 37 del Codice (cfr. anche provvedimento del Garante n. 1/2004 del 31 marzo 2004 recante i casi da sottrarre all'obbligo di notificazione, pubblicato sulla G. U. n. 81 del 6 aprile 2004 e disponibile sul sito dell'Autorità www.garanteprivacy.it (doc. web n. 852561));

b) alla predisposizione dell'informativa da fornire agli interessati (art. 13 del Codice);

c) all'acquisizione del consenso per i trattamenti di dati personali connessi all'erogazione delle prestazioni e dei servizi per svolgere attività di prevenzione, diagnosi, cura e riabilitazione (artt. 22, 26 e 76 del Codice);

d) per gli organismi sanitari pubblici, al rispetto delle disposizioni contenute nel regolamento per il trattamento dei dati sensibili per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione adottato ai sensi dell'art. 20 del Codice (cfr. Provv. del 30 giugno 2005);

e) al rispetto delle autorizzazioni generali rilasciate dal Garante ed, in particolare, dell'autorizzazione generale al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (artt. 26 e 76 del Codice);

f) alle misure di sicurezza (artt. 31-36 del Codice e allegato B) al Codice).

TUTTO CIÒ PREMESSO, IL GARANTE:

1. prescrive a tutti i titolari del trattamento di dati personali interessati in ambito sanitario, ai sensi dell'art. 154, comma 1, lett. c), del Codice di adottare, ove già non attuate, le misure necessarie od opportune al fine di rendere il trattamento dei medesimi dati conforme alle disposizioni vigenti, sulla base dei principi richiamati nel presente provvedimento e dei primi chiarimenti con esso forniti;

2. prescrive ai medesimi titolari, ai sensi dell'art. 154, comma 1, lett. c), del Codice di adottare comunque tutte le ulteriori misure per garantire, in materia di trattamento dei dati personali nell'ambito sanitario, il massimo rispetto del principio di dignità;

3. avvia una consultazione allo scopo di acquisire elementi di informazione e documentazione da parte di organismi sanitari, nonché di soggetti, portatori di interessi pubblici e privati e portatori di interessi diffusi, costituiti in associazioni e comitati, in ordine alle modalità di attuazione adottate ed alle problematiche riscontrate.

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 un importante provvedimento avente ad oggetto il rispetto della dignità personale nell'ambito delle strutture sanitarie, secondo quanto previsto dall'art. 83 del codice della privacy.

In attuazione delle linee guida e dei suggerimenti dell'Autorità, l'azienda impartisce le seguenti istruzioni a ogni operatore:

Rapporti di front-office

- **Modalità di chiamata degli interessati**

L'Azienda ha già adottato idonee misure a garanzia dell'ordine di precedenza degli interessati con riferimento al rapporto di front-office.
Considerato l'obbligo di procedere alla chiamata in occasione di attesa in spazi promiscui, prescindendo dalla individuazione nominativa dell'interessato, ogni responsabile di singola struttura deve adottare un sistema di chiamata numerico o altra soluzione (ad es. numero di prestazione o orario di appuntamento, ticket colorato, altro), che consenta di assicurare il rispetto della dignità del soggetto. Si consiglia, nel caso di ricorso al numero di chiamata, di rivolgersi al paziente utilizzando la seguente formula: "chi ha il numero …." piuttosto che "chi è il numero ….".

- **Distanza di cortesia**.

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.

- **Contatto con il pubblico.**

Il dialogo-colloquio tra personale dell'Azienda Sanitaria e Ospedaliera e gli utenti, qualora abbia ad oggetto informazioni inerenti lo stato di salute dell'interessato, e qualora avvenga in spazi od in situazioni ove vi è la presenza di altri soggetti, oltre l'utente interessato (ad esempio nelle stanze di degenza a più posti letto o nei punti ove vengono ritirati dagli interessati esami, referti etc., o presso le accettazioni e le segreterie delle Unità), deve essere improntato ad un criterio di prevenzione e prudenziale. Tale prudenza deve caratterizzare tutte le condizioni usuali di colloquio tra operatori sanitari nell'esercizio della propria professione: discussione di casi clinici durante il giro-visita, supervisione di casi in luoghi aperti all'utenza, consulenze specialistiche effettuate al letto di degenza, passaggi di consegne tra personale, comunicazioni di servizio effettuate mediante apparecchi telefonici portatili o meno non posizionati in luoghi protetti, informazioni fornite a frequentatori medici, consulenti.

Tutela della riservatezza nel caso di trasferimento della documentazione

- **Modalità di trasferimento interno della documentazione cartacea contenente dati di salute**.

Quando le cartelle cliniche e altra documentazione sanitaria devono essere trasferite da una struttura o da un ufficio presso altro luogo 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, sigillarne i lembi e apporre la propria firma per garantirne l'integrità.

- **Modalità di conservazione della documentazione cartacea negli archivi delle Strutture Operative**

I locali adibiti ad archivio all'interno di ciascuna Unità Operativa, contenenti documentazione con dati personali di natura sensibile, devono essere chiusi a chiave e le chiavi devono essere in possesso del personale autorizzato (accesso selezionato); si consiglia di predisporre un registro cartaceo o di adottare altra procedura di controllo, al fine di verificare l'identità di coloro che accedono all'archivio (nel registro, ove si provveda alla sua adozione, devono essere indicati le generalità di coloro che sono autorizzati, anche in via preventiva, ad accedere ai dati e alla documentazione, riportando i dati identificativi e la qualifica professionale rivestita.

Cautele per la tutela della riservatezza e la protezione dei dati degli assistiti

- **Modalità di esposizione delle tabelle presenza nei reparti di degenza**.

Le tabelle presenza dei degenti devono essere collocate in locali od aree riservate, visibili solamente da parte del personale autorizzato alla consultazione (ad esempio nella guardiola della caposala). Si devono evitare lavagne o altri dispositivi posti in zone aperte o accessibili al pubblico (corridoi, sale di attesa,…).

- **Richiesta di informazioni sulla presenza di un paziente.**

Nel caso venga chiesto se una persona è ricoverata o meno presso l'Ospedale, è possibile dare tale informazione se l'interessato non ha specificamente richiesto, al momento del suo ingresso nella struttura, che la sua presenza sia mantenuta anonima. Pertanto, ove il paziente non si pronunciasse, il personale è autorizzato a fornire tale informazione.

- **Richiesta di informazioni sullo stato di salute di un paziente ricoverato.**

Nel caso si presentino parenti, amici, conoscenti, che chiedono notizie inerenti allo stato di salute di un utente ricoverato (patologia, diagnosi, terapia etc), non è possibile fornire tali informazioni senza aver prima verificato, sull'apposito modulo di annotazione del consenso, quali sono i soggetti specificamente autorizzati dall'interessato a ricevere comunicazioni inerenti il suo stato di salute.

- **Religione e relative domande.**

Evitare, ove possibile, domande relative alla convinzione religiosa che è un dato sensibile non necessario ai fini della permanenza della persona stessa nell'Azienda. Sono da preferire forme alternative e indirette ad esempio: per stabilire la preferenza alimentare del paziente (nel caso specifico per evitare le portate a base di maiale) non domandare:
"A quale religione appartiene?" o "E' di religione ebraica?", ma usare forme indirette del tipo "Ha delle preferenze alimentari ?"

CAPITOLO 03
Decalogo per la sicurezza degli strumenti e la protezione dei dati personali

1 - Utilizzo del personal computer in dotazione

1) Utilizzare il pc in dotazione esclusivamente per ragioni di lavoro e per conto dell'azienda;
2) assicurare che quando siete al lavoro nessuno possa conoscere i dati che state digitando o i file su cui state lavorando, ponendo attenzione a posizionare il vostro 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 accesso è maggiormente attaccabile in quanto raggiungibile tramite la rete o direttamente sulla postazione di lavoro;
6) lasciare un computer acceso aumenta il rischio che un'interruzione dell'energia elettrica possa causare un danno;
7) non lasciare mai incustodito un notebook in ufficio o in viaggio (particolare attenzione deve essere riposta quando si viaggia sui mezzi pubblici);
8) durante gli spostamenti 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 proprio notebook.

2 - Password

1) La parola chiave (password), assegnata a ciascun incaricato, è composta da un minimo di otto caratteri o comunque dal numero massimo di caratteri consentito dal sistema;
2) la parola chiave deve essere prontamente sostituita dall'incaricato al primo utilizzo e deve essere modificata con cadenza almeno trimestrale;
3) la password non deve contenere riferimenti agevolmente riconducibile all'incaricato e deve essere generata preferibilmente senza un significato compiuto;

4) l'incaricato, nello scegliere la propria password, deve utilizzare anche caratteri speciali e lettere maiuscole e minuscole;

5) la parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;

6) l'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare;

7) fare attenzione a non essere "spiati" durante la digitazione di una password o qualunque codice di accesso;

8) prestare attenzione nella digitazione della propria password, per cui anche se si possiede una buona velocità cercare di leggere la tastiera;

9) non permettere l'uso del proprio account 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 pc 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 distrutti;
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 dell'amministratore di sistema, il software antivirus;
6) la posta elettronica viene filtrata in entrata da un apposito prodotto antivirus che pulisce gli eventuali allegati contenenti virus;
7) evitare di aprire messaggi provenienti da mittenti sconosciuti o sospetti e cancellarli immediatamente;
8) 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;
9) 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 dell'azienda, nella persona del Direttore responsabile del Dipartimento Interaziendale Information Technology (DIIT);
3) non installare da soli i software sul proprio pc, se non previa autorizzazione da parte del proprio responsabile di struttura;
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);
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 confidenzialità dei messaggi e dei contenuti;
4) si deve evitare di rispondere alla 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 e amministrativa aziendale;
8) mantenere costantemente attivo e aggiornato il programma antivirus per il controllo dei messaggi di posta elettronica inviati o ricevuti.

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) Assicuratevi che solo strumenti forniti o autorizzati dall'azienda vengano allacciati alla rete di comunicazione aziendale;
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.