Istruzioni per gli autorizzati al trattamento dei dati personali

SOMMARIO

1.1 PREMESSA

L'Azienda Ospedaliera S. Croce e Carle, titolare del trattamento dati, con Deliberazione del Direttore Generale ha individuato tutti i dipendenti dell'Azienda come autorizzati al trattamento dei dati effettuato nello svolgimento delle proprie funzioni.
Analogamente vengono individuati come autorizzati tutti i soggetti che instaurano rapporti di lavoro autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e altre forme di impiego che non comportano costituzione di un rapporto di lavoro subordinato all'atto della sottoscrizione della consulenza contratto; in generale sono autorizzati tutti i soggetti che accedono ai dati personali e sono preposti allo svolgimento delle operazioni di trattamento relative ai dati.

Il principio generale che ispira l'autorizzazione è di diligenza e correttezza. Gli autorizzati possono trattare esclusivamente i dati necessari per l'espletamento dell'attività affidata, secondo i compiti che sono individuati per la struttura di appartenenza o di riferimento nell'atto aziendale vigente. Ogni utilizzo dei dati in possesso dell'Azienda diverso da finalità strettamente professionali è espressamente vietato.

Ai sensi del Reg. UE 2016/679 e del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 e ss.mm.ii.) il trattamento dei dati personali deve avvenire nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona. In particolare devono essere particolarmente tutelati i dati relativi alla salute, i dati genetici e i dati biometrici. Nelle norme è inoltre previsto che sia obbligo di risarcimento del danno da parte di chi effettua un qualunque trattamento di dati personali a meno che provi di aver adottato tutte le misure idonee ad evitare il danno cagionato.

Le istruzioni e le regole comportamentali che vengono esposte di seguito sono finalizzate ad evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e informatico e all'immagine dell'Azienda: devono essere applicate dagli autorizzati ogni qualvolta trattano dei dati personali, su supporto cartaceo e/o informatico, di titolarità dell'Azienda Ospedaliera S. Croce e Carle; l'inosservanza delle stesse potrà comportare l'applicazione di sanzioni civili, penali, amministrative, disciplinari ai sensi di legge.

Queste istruzioni andranno eventualmente integrate da ulteriori istruzioni specifiche definite dai designati per situazioni particolari.
Inoltre costituiscono istruzioni le eventuali indicazioni specifiche fornite dalla Direzione Generale, dal Data Protection Officer; in particolare si segnalano gli avvisi di sicurezza e le istruzioni che la S.C.I. Sistema Informatico Direzionale (nel seguito SID) distribuisce periodicamente.
Al fine di migliorare costantemente il livello di sicurezza, è fatto obbligo per tutti gli autorizzati la periodica lettura e consultazione degli avvisi di sicurezza di cui sopra.
I documenti citati, nonché altre informazioni in materia di protezione dei dati, sono disponibili sulla intranet aziendale.

***DEFINIZIONI*:**
Al fine di facilitare comportamenti corretti, è innanzitutto necessario condividere il significato di alcuni termini connessi al trattamento dei dati personali. Di seguito un breve glossario di quelli più utili:

- ***trattamento***: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione,

diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- ***dato personale*:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- ***dati particolari*:** i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- ***dati relativi alla salute***: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- ***interessato***: la persona fisica cui si riferiscono i dati personali;
- ***titolare del trattamento***: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che singolarmente o insieme ad altri, determinate finalità e i mezzi del trattamento di dati personali;
- ***designati:*** persone fisiche che operano sotto l'autorità del titolare (Azienda Ospedaliera S. Croce e Carle) e alle quali sono stati attribuiti specifici compiti e funzioni connessi al trattamento di dati personali.

Nell'ambito dell'attività lavorativa, il dipendente deve assicurarsi che i dati personali siano:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
f) elaborati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).

1.2 UTILIZZO E CONSERVAZIONE DEI DATI

Gli strumenti di lavoro messi a disposizione dell'Azienda Ospedaliera S. Croce e Carle sono finalizzati all'uso professionale e destinati all'adempimento delle mansioni assegnate ed è responsabilità dei singoli assegnatari custodirli in modo appropriato e diligente al fine di evitare, per quanto possibile, il furto, l'appropriazione o anche solo l'utilizzo da parte di terzi non autorizzati. E' indispensabile segnalare prontamente alla struttura competente il danneggiamento, lo smarrimento o il furto di tali strumenti.

Per l'utilizzo dei dispositivi elettronici, della posta elettronica e di internet si deve far riferimento al Regolamento approvato (e successive modifiche disponibili sul sito intranet) che è da considerarsi come parte integrante delle presenti istruzioni. Si riporta nel seguito una sintesi delle istruzioni, a titolo esemplificativo e non esaustivo:

a) Non è consentito:
   - **Utilizzare la stessa password impiegata per l'accesso alla rete aziendale anche per accedere a servizi esterni** (cloud, mail personali, social network, …);
   - Utilizzare la mail aziendale per accedere a servizi esterni non attinenti l'attività lavorativa (es. cloud, mail personali, social network, …);
   - Utilizzare funzioni e tecniche di condivisione dei propri archivi (al di fuori di quelli predisposti dal SID);
   - Memorizzare dati aziendali su piattaforme in CLOUD non autorizzate dall'Azienda;
   - Aprire canali informativi telematici non autorizzati da e verso l'esterno dell'Azienda in qualsiasi forma (ad es. collegamento via modem o chiavette Internet wireless o tramite Internet), compresi sistemi di telecontrollo e condivisione del desktop (es. Teamviewer) eventualmente richiesti da fornitori esterni;
   - Modificare la configurazione hardware/software della postazione di lavoro, installare qualsiasi tipo di software se non autorizzato dal SID, alterare la configurazione di rete, disattivare anche temporaneamente l'antivirus;
   - L'accesso a social network (es. Facebook, Twitter, YouTube, …), chat esterne (es. Messenger, Whatsapp, …), giochi online ed altre applicazioni online se non finalizzate all'attività lavorativa. Anche in quest'ultimo caso, non è comunque consentito l'utilizzo di social network o chat per trattare o scambiare informazioni tutelate dalla normativa sulla Protezione dei Dati;
   - L'accesso a siti internet i cui certificati di protezione non siano corrispondenti ai livelli minimi di sicurezza (es. certificati scaduti o non rilasciati da Certification Authorities ufficiali);
   - Memorizzare dati personali (anche relativi alla salute dei pazienti) su dispositivi rimovibili (es. CD/DVD, chiavette USB, …) e sulla propria postazione di lavoro, salvo nei casi espressamente autorizzati dal SID. Nel caso in cui sia assolutamente necessario, il supporto deve essere protetto mediante password o meccanismi di cifratura e deve essere garantito il salvataggio periodico dei dati e la sua custodia;

b) E' obbligatorio:
   - Richiedere il collegamento alla rete aziendale di qualunque postazione di lavoro o dispositivo esclusivamente agli operatori autorizzati del SID (mediante portale interno delle richieste) che operano seguendo procedure standard di configurazione, garantendo la sicurezza degli accessi e la protezione dei sistemi;
   - Evitare di aprire messaggi di posta elettronica provenienti da soggetti non legati all'attività lavorativa o sconosciuti;
   - Evitare di visitare siti i cui link sono contenuti nei messaggi di posta elettronica sospetti;
   - Evitare di aprire allegati di cui non si conosce il contenuto;
   - Diffidare di messaggi di posta elettronica provenienti da persone sconosciute, scritti in lingua straniera o che richiedono di eseguire programmi cliccando su appositi link;

c) Dispositivi mobili aziendali:
   - E' vietato collegarsi a reti wifi pubbliche o non protette da sistemi di sicurezza (quali password di accesso o altro);
   - E' obbligatorio, qualora siano memorizzati anche temporaneamente dati aziendali e/o personali sulla postazione, attivare la cifratura dei dati;

- Porre ulteriore attenzione ai messaggi di posta elettronica, ai link in essi contenuti e in generale a quali siti internet vengono consultati in relazione al fatto che le connessioni Internet esterne all'Azienda non garantiscono un'adeguata sicurezza;
- Limitare l'utilizzo di protocolli di comunicazione non sicuri (es. bluetooth) al tempo strettamente necessario;

d) Dispositivi personali:
   - Per motivi di sicurezza non è consentita la connessione di dispositivi personali alla rete aziendale;
   - La connessione al wifi pubblico disponibile nelle sedi aziendali non è considerato accesso alla rete aziendale;
   - L'utilizzo di dispositivi personali per accedere a servizi aziendali tramite Internet (es. posta elettronica, portale del dipendente, …) è ammesso purché:
     - Non vengano memorizzati sui dispositivi personali documenti aziendali che presentino un rischio per i diritti e le libertà delle persone secondo il Regolamento Europeo per la Protezione dei Dati (GDPR);
     - Non vengano trasmessi dati personali aziendali su cloud o social network.

E' altresì doveroso salvaguardare l'integrità e la sicurezza dei dati e dei documenti trattati o comunque accessibili attraverso gli strumenti di cui sopra, prestando la massima attenzione per le informazioni a carattere riservato e particolare.

e) I dati devono essere conservati in luoghi sicuri, con accesso protetto:
   - è necessario assicurarsi che l'ufficio in cui sono conservate le banche dati sia sempre **custodito** durante l'orario di apertura;
   - in caso di allontanamento, anche temporaneo, dal posto di lavoro, l'autorizzato dovrà verificare che non vi sia la possibilità da parte di terzi, anche se dipendenti, di accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento;
   - **fuori orario di apertura o comunque in assenza di autorizzati**:
     - le banche dati, se su supporto cartaceo o su floppy disk, CD, DVD o memoria USB, devono essere custodite in armadi chiusi a chiave ovvero, in mancanza di serratura, deve essere chiuso a chiave lo stesso locale adibito ad archivio;
     - il P.C. su cui sono memorizzate le banche dati deve essere spento e, ove non sia possibile la chiusura a chiave dello sportellino dell'interruttore di accensione dello stesso ovvero non sia prevista un password di accesso al programma, deve essere chiuso a chiave il locale ove è ubicato il P.C.;
     - le chiavi degli armadi, dei locali ovvero dei P.C. ove sono custodite le banche dati devono essere depositate in luogo sicuro; una copia di dette chiavi deve essere custodita dal responsabile dell'ufficio o dal suo delegato;

f) I supporti (digitali o cartacei) per la memorizzazione di dati personali devono recare indicazioni in ordine almeno ai dati contenuti ed al periodo di riferimento.

Si precisano inoltre le seguenti istruzioni:
- Particolare attenzione va posta verso i dispositivi mobili, per loro natura estremamente vulnerabile, che sono veri e propri punti di accesso al Sistema Informativo; è fondamentale proteggerne l'accesso mediante gli strumenti messi a disposizione dal loro sistema operativo, cambiando regolarmente le password.
- Gli autorizzati al trattamento devono sempre utilizzare, per la memorizzazione, gli strumenti messi a disposizione dall'Azienda Ospedaliera S. Croce e Carle: in caso di necessità (anche solo temporanea) di mantenere per i fini di lavorazione una copia delle informazioni off-line

(sul disco interno delle postazioni di lavoro), la copia locale deve essere cifrata (es. tramite funzioni di cifratura delle applicazioni) ed eliminata al termine della lavorazione. E' buona regola la periodica pulizia degli spazi di memorizzazione delle unità di rete, dell'hard-disk della propria postazione di lavoro e della casella di posta, con cancellazione di file ed e-mail obsoleti e inutili contenenti dati personali, ed evitando la duplicazione dei dati memorizzati. La medesima attenzione dovrà essere riservata ai documenti cartacei contenenti dati personali che, per quanto possibile, non devono essere lasciati sulla scrivania o sui davanzali delle finestre o comunque in vista, ma riposti, quando non utilizzati e comunque al termine dell'attività lavorativa, negli appositi archivi correnti come da misure di sicurezza.

- In nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare.
- La documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli autorizzati, deve comunque essere rimossa al termine dell'orario di lavoro.
- L'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti.
- I supporti devono essere archiviati in ambiente ad accesso controllato.
- I documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete).
- Il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro.
- Cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro.
- E' severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.
- All'interessato deve essere garantito l'esercizio dei diritti sui propri dati che il Reg. UE 2016/679 gli riconosce (es. di accesso, di rettifica, di opposizione,…) per cui sono stabilite apposite procedure aziendali: ogni autorizzato al trattamento deve collaborare affinché tali procedure si svolgano secondo le tempistiche e le modalità stabilite dall'Azienda.

1.3 COMUNICAZIONE DI DATI PERSONALI

a) **Comunicazione tra uffici dell'Azienda**: occorre trasmettere i soli dati necessari alle finalità e attinenti/necessari ai trattamenti attuati per cui sono stati richiesti;
b) **comunicazione al di fuori dell'Azienda:** la comunicazione di dati al di fuori dell'Azienda deve essere autorizzata dal responsabile della struttura o dal designato o dal titolare del trattamento;
c) **trasmissione e comunicazione di "dati personali":** la trasmissione e la comunicazione di dati "personali" mediante posta ordinaria (cartacea), all'interno o all'esterno dell'Azienda, deve avvenire sempre mediante supporti cartacei o digitali confezionati in buste o pacchi chiusi. Nel caso di dati <personali particolari>, sulla confezione o su un documento accompagnatorio, deve essere indicata la dicitura "**DATI RISERVATI"**;
d) **accessi impropri**: onde evitare accessi impropri ai dati personali è opportuno elaborare gli stessi al riparo da sguardi indiscreti, soprattutto allorché si tratti di dati particolari;
e) **distruzione documenti non soggetti alla conservazione a norma di legge:** la distruzione di documenti contenenti dati aventi carattere strettamente personale deve avvenire in modo da rendere illeggibile il documento stesso (si consiglia di strappare in più pezzi il supporto cartaceo ovvero di formattare il supporto; i supporti rimovibili contenenti dati particolari o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati

da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili;

f) art. 12 del DPR 16 aprile 2013 n. 62 Regolamento recante codice di comportamento dei dipendenti pubblici prevede "*Il dipendente osserva il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali e, qualora sia richiesto oralmente di fornire informazioni, atti, documenti non accessibili tutelati dal segreto di ufficio o dalle disposizioni in materia di dati personali, informa il richiedente dei motivi che ostacolano all'accoglimento della richiesta*" (cfr. Codice di Comportamento per il personale dell'Azienda Ospedaliera S. Croce e Carle);

g) Per la comunicazione dei dati attraverso strumenti elettronici (email) si rimanda alle regole già definite nel citato Regolamento aziendale.
La trasmissione tramite posta elettronica su Internet di documenti contenenti dati particolari è consentita solo con l'impiego di caselle di posta sicura certificata o sistemi di crittografia certificati secondo standard stabiliti dall'Agenzia per l'Italia Digitale. Per la consegna tramite web o posta elettronica o posta elettronica certificata o domicilio digitale del cittadino o tramite supporto elettronico o tramite Fascicolo Sanitario Elettronico (FSE) di documentazione sanitaria è necessario attenersi a quanto stabilito dal D.P.C.M. 8 agosto 2013 e s.m.i.

h) Internet: il traffico verso internet viene protetto da specifici sistemi di sicurezza che abilitano il traffico Internet verso la rete esterna bloccando accessi non autorizzati da Internet verso la rete aziendale.
Per motivi di sicurezza non è permessa l'installazione di un modem, se non in casi eccezionali di effettiva necessità, previa autorizzazione da parte del SID.

i) E' vietato l'utilizzo ed il collegamento alla rete aziendale di apparecchiature non assegnate o autorizzate dal SID.

1.4 CREAZIONE DI BANCHE DATI

La creazione di banche dati deve essere autorizzata dai designati del trattamento previa analisi tecnica e stesura del piano di attività in stretta collaborazione con il direttore della S.C.I. Sistema Informativo Direzionale (SID).

1.5 ULTERIORI MISURE PER IL RISPETTO DEI DIRITTI DEGLI UTENTI

Al fine di garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati e del segreto professionale, nel caso in cui l'autorizzato (appartenente al ruolo sanitario o amministrativo) tratti dati personali e dati idonei a rivelare lo stato di salute degli utenti (assistiti, ricoverati, etc.) è necessario che adotti le misure qui di seguito (che fanno tra l'altro riferimento al Provvedimento del Garante per la protezione dei dati personali "*Strutture sanitarie rispetto della dignità*" del 09.11.2005 a disposizione sulla intranet aziendale).

1. Rispetto della dignità dell'interessato quando viene erogata una prestazione sanitaria
L'Azienda Ospedaliera S. Croce e Carle in qualità di titolare del trattamento personale dei dati deve **garantire** il pieno rispetto della **dignità** del paziente. La tutela della dignità deve essere garantita **con particolare riguardo** alle fasce deboli quali i disabili, 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-*).

2. Rispetto della riservatezza nei colloqui e nelle prestazioni sanitarie

É doveroso adottare idonee cautele (distanze di cortesia etc.) in relazione allo svolgimento di colloqui (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).

In tutti i casi in cui si effettua il trattamento di dati sanitari (es. operazioni di sportello, acquisizione di informazioni sullo stato di salute), è necessario rispettare i principi di confidenzialità e di riservatezza dell'interessato predisponendo idonee distanze di cortesia. Vanno in questa prospettiva prefigurate appropriate soluzioni, sensibilizzando gli utenti con idonei inviti, segnali o cartelli.

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).

3. Notizie su prestazioni di pronto soccorso o inerenti la dislocazione dei pazienti nei reparti

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 indicazioni specifiche o contrarie dell'assistito. 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 circa la dislocazione dei degenti nei reparti può essere fornita, fatta salva eventuale volontà contraria dell'utente. 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. 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.
Non devono essere 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).
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, è necessario adottare apposite cautele (utilizzo dei soli dati necessari per l'espletamento dell'attività) anche nel rilascio di 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).

4. Comunicazione dei dati idonei a rivelare lo stato di salute
Le informazioni sullo stato di salute dell'interessato possono essere comunicate solo per il tramite di un medico o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente (ad es. un infermiere autorizzato per iscritto dal titolare o dal responsabile). Nel caso in cui l'interessato riceva una comunicazione dalla struttura sanitaria che documenti gli esiti di esami clinici effettuati, l'intermediazione deve essere soddisfatta accompagnando un giudizio scritto con la disponibilità del medico a fornire ulteriori indicazioni a richiesta.
La consegna a terzi dei documenti contenenti dati idonei a rivelare lo stato di salute dell'interessato (es. referti diagnostici, certificazioni rilasciate dai laboratori di analisi) può essere fatta solo se chi ritira ha una delega scritta corredata dalla fotocopia del documento di identità del delegante. La consegna della documentazione deve avvenire in busta chiusa.

5. Rispetto del segreto d'ufficio, professionale
L'autorizzato al trattamento è tenuto a rispettare il segreto d'ufficio, il segreto professionale. Colui che non è tenuto per legge al segreto professionale (ad es. personale tecnico e ausiliario) deve comportarsi come se fosse tenuto al rispetto degli obblighi derivanti dal suddetto segreto.

1.6 COMPORTAMENTO IN CASO DI VIOLAZIONE DELLA SICUREZZA

La "violazione" è definita all'art. 4 par. 12 del Reg. UE 2016/679 come "la violazione di sicurezza che comporta accidentalmente in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" (DATA BREACH). Non appena viene a conoscenza di una violazione di dati personali, al momento del verificarsi del fatto o della sua scoperta, tutti gli autorizzati al trattamento devono segnalarlo al proprio Responsabile diretto al fine di avviare la procedura definita nel sistema aziendale come Procedura "DATA BREACH".
Esempi, a puro titolo esemplificativo, di eventi che possono comportare un data breach: pubblicazione di un atto deliberativo nella sua interezza senza omissione di dati personali/particolari; inoltro di messaggi contenenti dati personali/particolari a soggetti non interessati al trattamento; abbandono della postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, disattivare le procedure sulla risorsa informatica utilizzata, ecc..) e vi è evidenza che terzi abbiano avuto accesso alle informazioni; perdita della chiave di decriptazione di dati crittografati in modo sicuro (se l'unica copia a disposizione); cancellazione dei dati in modo accidentale o da parte di soggetti non autorizzati (senza possibilità di recupero); data exfiltration (copia o trasferimento non autorizzati di dati); ransomware/malware; distruzione accidentale di un supporto di memorizzazione; smarrimento, furto di PC o server; smarrimento, furto di dispositivo mobile (smartphone, USB KEY, CD/DVD HD, etc.); smarrimento, furto o

distruzione accidentale di documenti o aggregazioni documentali negli archivi cartacei (correnti o di deposito).

ELENCO DI DISTRIBUZIONE

Tutti i dipendenti dell'Azienda.

Tutti i soggetti che instaurano rapporti di lavoro autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e altre forme di impiego che non comportano costituzione di un rapporto di lavoro subordinato all'atto della sottoscrizione della consulenza contratto; in generale sono autorizzati tutti i soggetti che accedono ai dati personali e sono preposti allo svolgimento delle operazioni di trattamento relative ai dati.

Diffusione: pagine web intranet e internet dedicate alla protezione dati personali; pubblicazione nella sezione *Comunicazioni* del Portale del dipendente; per il nuovo personale con la sottoscrizione del contratto di lavoro.