REGIONE DEL VENETO
AZIENDA OSPEDALIERA DI PADOVA

Delibera del Direttore Generale n. 262 del 07/03/2019

OGGETTO: Regolamento UE 2016/679 - ridefinizione dei profili di responsabilità in tema di protezione dei dati personali e nuove modalità di designazione dei soggetti Delegati Privacy (ex Responsabili) e Autorizzati al trattamento di dati personali (ex incaricati).

NOTE TRASPARENZA: con il presente provvedimento si provvede a ridefinire, a seguito delle nuove disposizioni europee e italiane in materia, i profili di responsabilità in tema di protezione dei dati personali e le nuove modalità di designazione dei soggetti Delegati Privacy (ex Responsabili interni) e Autorizzati (ex Incaricati) al trattamento di dati personali, precedentemente definiti con deliberazione del Direttore Generale n. 231 del 30/03/2006.

Il Sostituto Responsabile della **UOC Affari Generali e Legali** riferisce:

Il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (General Data Protection Regulation o GDPR), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, nell'affrontare il tema della tutela dei dati personali, attraverso un approccio basato principalmente sulla valutazione dei rischi sui diritti e le libertà degli interessati, attribuisce al Titolare del trattamento (ovvero a questa Azienda Ospedaliera) il potere di adottare le misure che ritiene più idonee ed opportune per garantire la protezione dati personali;
Il "sistema privacy " delineato dal GDPR, e dal D.Lgs 196/2003 novellato dal D.Lgs 101/2018 (entrato in vigore il 19/09/2019), contenente disposizioni di adeguamento della normativa nazionale al normativa europea, implica la necessità di infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti i trattamenti, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero asset organizzativo, con particolare attenzione alle categorie particolari di dati (ex sensibili), tra i quali quelli relativi alla salute;
In particolare si richiama la principale novità introdotta dal GDPR, ovvero il principio di "responsabilizzazione" (cd. *Accountability* nell'accezione inglese) che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate ed efficaci in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative che siano concretamente dimostrabili e conformi alle disposizioni europee (principio

della "conformità" o *compliance* nell'accezione inglese);vi è quindi l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento UE, così da poterne dare conto, in qualsiasi momento, verso l'esterno (il termine *Accountability*, infatti, rinvia letteralmente al concetto di "resa di conto").

Questa Azienda Ospedaliera, nella persona del Suo Direttore Generale, ha fatto proprio l'approccio del legislatore europeo relativo all' *Accountability* ed alla *compliance,* adottando con anticipo rispetto all'applicazione del GDPR, la Deliberazione n. 537 del 24/04/2018 ad oggetto*"Adempimenti da attuare per dare corretta applicazione alla normativa del nuovo Regolamento Europeo 679/2016 sulla Data Protection (GDPR -General Data Protection Regulation)"*.

Con detta deliberazione si è provveduto ad approvare, quale strumento programmatico, la Relazione Tecnica contenente le azioni di carattere organizzativo, gestionale, tecnologico e documentale volte ad ottemperare, dando avvio, nell'ambito di questa Azienda Ospedaliera, al percorso per ottemperare ai precetti della normativa europea e italiana in materia.

A seguito di questa delibera, nel corso del 2018, sono state approvate ulteriori deliberazioni, volte a proseguire il percorso di adeguamento di questa Azienda alle nuove disposizioni normative europee e nazionali, secondo le linee di indirizzo e di coordinamento fornite dall'Azienda Zero (ente di governance della sanità veneta) al fine di favorire, in modo omogeneo, l'applicazione dei complessi adempimenti previsti dal GDPR presso le diverse realtà sanitarie dell'intero territorio regionale.

Si ricordano la deliberazione del Direttore Generale n. 659 del 22/05/2018 con la quale è stato approvato lo schema di convenzione con Arsenàl.IT-Centro Veneto Ricerca e Innovazione per la Sanità Digitale - per l'attività di cui al "Progetto tecnico e proposta economica per supporto e adeguamento al GDPR e attività per l'espletamento del ruolo di Responsabile della Protezione dei Dati (RPD) unico per tutte le Aziende Sanitarie del Veneto"; la deliberazione n. 660 del 22/05/2018 di designazione del Responsabile della Protezione dei Dati personali (RPD), ai sensi dell 'art. 37 del Regolamento UE 2016/679; la deliberazione n. 846 del 06/07/2018 con la quale è stato costituito il Gruppo privacy aziendale per il supporto all'RPD e al Board/RPD, nonché per coadiuvare il Referente Privacy aziendale nell'attuazione degli adempimenti di adeguamento al Regolamento UE 201/679 e la deliberazione n. 1501 del 10/12/2018 contenente gli adempimenti di carattere documentale: approvazione modelli di informativa (varie), consenso (se necessario) e di schema di accordo per la nomina del Responsabile Esterno del Trattamento dei Dati Personali.

Con successiva nota prot. 16336 del 17/12/2018 l'Azienda Zero, sempre allo scopo di omogeneizzare all'interno del territorio regionale la

complessa gestione degli adempimenti previsti dal GDPR e dalle recenti novità di cui al D.Lgs 101 del 10/10/2018, che hanno novellato il D.Lgs 196/2003, ha trasmesso a tutte le aziende sanitarie ed ospedaliere della Regione Veneto, tra gli altri, i modelli "standard", da adeguare alle specifiche esigenze organizzative aziendali, di nomina Delegati interni al trattamento (**Delegati Privacy –** ex Responsabili interni del trattamento) e di **"Autorizzati al trattamento"** (ex incaricati) e **istruzioni operative da fornire agli autorizzati al trattamento.**

Si evidenzia, infatti, che, con riferimento ai soggetti protagonisti del trattamento dei dati personali, il GDPR:

- disciplina, rafforzandola, la figura del "Titolare del trattamento", quale soggetto che determina le finalità e i mezzi dei trattamenti dei dati personali effettuati nel proprio ambito (nel caso l'Azienda Ospedaliera di Padova) e del "Responsabile del trattamento", riferendosi con quest'ultima espressione in specifico ai soggetti - esterni alla organizzazione - che trattano dati personali "per conto del titolare del trattamento" con riferimento ai fornitori di servizi. (c.d . Outsourcing);
- non prevede più, espressamente, le figure del "Responsabile [interno] del trattamento" e dell'Incaricato" del trattamento (come in precedenza individuati, ai sensi degli artt. 29 e 30 del D.L.gs 196/2003 – Codice Privacy, con deliberazione del Direttore Generale n. 231 del 30/03/2006), tuttavia non ne esclude la effettiva designazione soprattutto all'interno di un'organizzazione complessa come quella di un'azienda sanitaria di grandi dimensioni, consentendo che tali nomine contribuiscano a meglio delineare i singoli ambiti di intervento, nonché a monitorare le attività di trattamento dei dati personali svolte nell'ambito delle singole Unità Operative.

Il Titolare, pertanto, anche alla luce del nuovo principio di *Accountability*, può continuare ad avvalersi di un'adeguata ed efficace articolazione dei presidi e delle responsabilità a livello organizzativo mediante un sistema di deleghe di funzioni che risponda alle specifiche esigenze operative dei servizi e all'esigenza di disporre di una rete di indirizzo e di governo più prossima alle strutture produttive così da rendere più efficace e tempestiva sia l'organizzazione che la sorveglianza della gestione dei dati di competenza, nonchè la tempestiva segnalazione al Titolare di eventuali violazioni dei dati (data breach).

Il Titolare del trattamento dei dati, designa, quindi, i Direttori di Unità Operativa Complessa e i Responsabili di Unità Operativa Semplice Dipartimentale, nonché il Responsabile dei servizi informativi che forniscono per esperienza, capacità e affidabilità idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di protezione dei dati personali, ivi compreso il profilo relativo alla sicurezza, quali Delegati interni al trattamento dei dati (di seguito **Delegati Privacy**) provvedendo a conferire loro, ai sensi dell'art.2 quaterdecies, comma 1 del D.Lgs 196/2003 modificato e integrato dal D.Lgs 101/2018, con specifico atto

scritto, le deleghe relative all'esercizio di funzioni di direzione, di coordinamento e di controllo delle attività di trattamento dei dati personali svolte nell'ambito delle attività di competenza delle rispettive Unità Operative. Ciò in virtù e nei limiti dei poteri di organizzazione, gestione e controllo ai medesimi conferiti da questa Azienda Ospedaliera.
La UOC Risorse Umane provvederà, in ogni atto futuro, successivo all'adozione del presente Atto, avente ad oggetto il conferimento di incarico dirigenziale di Unità Operativa Complessa e di Unità Operativa Semplice Dipartimentale, ad inserire nel contratto di lavoro, espressamente, la nomina di "Delegato Privacy" e a consegnare all'atto della sottoscrizione del contratto stesso la delega al trattamento dei dati personali di cui il dipendente prenderà atto sottoscrivendo per ricevuta.
Per coloro che, alla data di adozione del presente provvedimento, ricoprono già l'incarico di Direttore/Responsabile di UOC/UOSD, l'individuazione quale Delegato Privacy s'intende formalizzata con apposita comunicazione, a cura della UOC Affari Generali e Legali.
Il Titolare, inoltre, con il presente provvedimento, designa ciascun dipendente, sia a tempo indeterminato che determinato, personale universitario in convenzione, nonché tutte le persone fisiche che a vario titolo prestano temporaneamente la loro attività all'interno delle varie strutture aziendali (specialisti ambulatoriali interni, titolari di incarico libero professionali, di borse di studio, di collaborazioni occasionali, di co.co.co, di contratto di prestazione d'opera, frequentatori, tirocinanti e frequenze extra rete formativa e volontari) dell'Azienda Ospedaliera, quali **Autorizzati al trattamento dei dati** (artt. 4 n. 10, art. 29 e 32 comma 4 del GDPR), ex incaricati, effettuato nell'espletamento delle loro mansioni, svolte nell'ambito delle attività di competenza della Unità Operativa Complessa o Semplice Dipartimentale alla quale sono stati formalmente assegnati.
Gli Autorizzati al trattamento dei dati dovranno attenersi con scrupolo e diligenza alle **istruzioni operative di cui all'All. 1,** al presente provvedimento**.** Gli Autorizzati che svolgono attività di trattamento dei dati all'interno delle Unità Operative che erogano prestazioni sanitarie di prevenzione diagnosi cura e riabilitazione, dovranno, altresì**,** attenersi con scrupolo e diligenza alle **istruzioni operative ulteriori e specifiche (All. 2)** al presente provvedimento.
Le suddette istruzioni sono impartite dal Titolare, e dovranno essere fornite agli Autorizzati dal Delegato Privacy della UOC/UOSD, alla quale la persona afferisce, che deve assicurarne l'attuazione e il rispetto.
Gli Autorizzati dovranno, inoltre, rispettare ogni altra istruzione scritta/verbale impartita loro dal Delegato Privacy Direttore/Responsabile della UOC/UOSD presso la quale gli stessi svolgeranno la propria attività.
Sempre nel rispetto del principio di *Accountability* il Titolare provvederà progressivamente a mettere in atto un sistema formale di distribuzione dei compiti e delle responsabilità in materia di trattamento dei dati

individuando per iscritto il tipo di trattamento consentito all'Autorizzato, in base al suo specifico profilo professionale, al fine di meglio delineare, in ossequio alle nuove attribuzioni di compiti e funzioni derivanti dal GDPR, i singoli ambiti di trattamento, al fine di strutturare un sistema privacy atto ad infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti i trattamenti, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero asset organizzativo, con specifica attenzione alle categorie particolari di dati, tra i quali quelli relativi alla salute.
La UOC Risorse Umane provvederà, dall'adozione del presente provvedimento, a predisporre il contratto di lavoro o di incarico, di personale con funzioni diverse da quelle di Direzione di Unità Operativa Complessa o Semplice Dipartimentale, mediante l'inserimento di un'apposita clausola che specifichi l'individuazione del soggetto quale Autorizzato al trattamento dei dati in relazione alle funzioni di competenza derivanti dal rapporto giuridico esistente con l'Azienda e a comunicare, nelle more della definizione di un sistema automatizzato, al Servizio Sistemi Informativi ogni spostamento interno, cessazione o altra variazione del predetto rapporto giuridico, che incida sulla figura di Autorizzato, per il blocco delle specifiche autorizzazioni precedentemente rilasciate per il trattamento dei dati.
Per coloro che, alla data di entrata in vigore del presente Regolamento, risultano avere già in atto un rapporto giuridico con l'Azienda, l'individuazione, quale Autorizzato al trattamento dei dati s'intende, formalizzata, nelle more della definizione di un sistema automatizzato, con la pubblicazione della presente delibera nel sito web aziendale nell'apposita sezione intranet ed internet, al fine di darne massima conoscibilità a tutti gli operatori aziendali.
Alla luce di quanto sopra argomentato, si rappresenta, pertanto, che l'Azienda, al fine di presidiare il "sistema privacy", ha adeguato, a seguito delle intervenute modifiche normative illustrate, la propria organizzazione interna, articolata sui diversi livelli di responsabilità, che oggi si può riassumere come segue:
- Responsabile della protezione dei dati (RPD) – c.d. Data Protection Officer;
- Referente privacy aziendale - Responsabile UOC Affari Generali e Legali;
- Gruppo Privacy aziendale (composto dal Referente privacy aziendale e da personale esperto in materia, afferente alle seguenti Unità Operative: Direzione Medica – Età Adulta; Direzione Professioni Sanitarie; Informatica ; Comunicazione e Rapporti con i Cittadini e Affari Generali e Legali);
- Delegati interni di trattamento dei dati personali "Delegati Privacy" (ex Responsabili interni): Direttori di Struttura Complessa, Responsabili di Struttura Semplice Dipartimentale dell'Azienda;

- Delegato interno della sicurezza del sistema informativo automatizzato: Responsabile dei sistemi informativi;
- Autorizzati al trattamento dei dati personali (ex incaricati): tutte le persone fisiche che a vario titolo svolgono attività all'interno delle varie strutture operative aziendali, come sopra individuati.

I Delegati Privacy, nell'ambito dei compiti e delle funzioni connessi al trattamento dei dati personali effettuato per lo svolgimento delle attività e delle competenze formalmente attribuite alla loro Struttura dovranno attenersi ai seguenti compiti la cui elencazione non può comunque ritenersi esauriente rispetto a tutte le attività e gli adempimenti connessi ad una compiuta e corretta attività di protezione dei dati:

a. indirizzare le attività di gestione e adempimento degli obblighi previsti dal GDPR e dal D.Lgs 196/2003, così come modificato dal D.Lgs 101/2018, nell'ambito delle attività di competenza dell'UOC/UOSD, definendole in coerenza con le direttive e prassi aziendali;
b. assicurare che le operazioni di trattamento dei dati personali siano effettuate, nell'ambito dell'UOC/UOSD di competenza, esclusivamente per lo svolgimento delle attività e compiti assegnati e nel pieno rispetto delle disposizioni del GDPR, del D.Lgs 196/2003, così come modificato dal D.Lgs 101/2018, delle istruzioni impartite dal Titolare e della prassi aziendale;
c. censire e monitorare i trattamenti di dati effettuati nell'UOC/UOSD di riferimento, nonché gli archivi e le banche di dati gestite nell'ambito dell'UOC/UOSD medesima, collaborando, per quanto di competenza, a fornire al sistema informativo aziendale e all'Ufficio Privacy Aziendale le informazioni necessarie per la costituzione ed aggiornamento (inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti), del registro dei trattamenti ex art. 30 del GDPR ed allo svolgimento delle correlate analisi dei rischi;
d. verificare gli adempimenti da porre in essere nell'ambito delle attività di competenza e collaborare alle attività svolte dall'Azienda in osservanza del GDPR, predisponendo i relativi atti, documenti, modulistiche anche contrattuali riguardanti i principali adempimenti privacy (es.: informativa e, ove necessario, consenso, nomina responsabile esterno) di competenza della relativa UOC/UOSD nonché le correlate comunicazioni interne ed esterne, ed assicurando la loro adozione, conservazione, aggiornamento e circolazione nell'ambito della struttura di competenza;
e. assicurare il rispetto, nell'ambito dell'UOC/UOSD e da parte del personale autorizzato al trattamento dei dati, delle adeguate misure organizzative e tecniche previste in adempimento al GDPR ed al D.Lgs 196/2003, così come modificato dal D.Lgs 101/2018, nonché delle politiche, istruzioni e misure aziendali di sicurezza dei dati,

segnalando all' UOC Risorse Umane, alla UOC Informatica, alla UOC Affari Generali e Legali e al Responsabile della protezione dei dati (RPD) competenti in materia di privacy, ognuno per la parte di propria competenza, eventuali esigenze o problematiche in proposito;

f. curare l'osservanza, per quanto di competenza, delle misure organizzative, tecniche e di sicurezza aziendali, in riferimento sia agli strumenti e sistemi informatici in uso, sia agli archivi e documenti cartacei direttamente gestiti, segnalando, al Responsabile dei sistemi informativi e alla UOC Affari Generali e Legali, i casi in cui, a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi come incendi o altre calamità, si dovessero verificare con la perdita, la distruzione o la diffusione indebita di dati personali trattati eventuali casi di violazione della sicurezza dei dati personali (c.d. "data breach");
g. segnalare o dare impulso alla procedura di valutazione d'impatto sulla protezione dei dati personali, laddove una nuova attività di trattamento dati o la modifica di un'attività di trattamento in essere preveda l'uso di nuove tecnologie e/o presenti un rischio elevato per i diritti degli interessati (art. 35 del GDPR), richiedendo, se del caso, il supporto consultivo del Responsabile della protezione dei dati (RPD) e/o della UOC Informatica e della UOC Affari Generali e Legali;
h. **individuare, consegnare e far sottoscrivere**, alle persone Autorizzate al trattamento dei dati personali, ovvero alle persone fisiche che a vario titolo prestano la loro attività, anche temporanea, all'interno della UOC/UOSD, **le istruzioni operative (All. 1 e All.2)** conservandone copia da esibire, su richiesta, alla UOC Affari Generali e Legali in caso di controlli del Responsabile per la Protezione dei dati (RPD) e/o del Garante Privacy, e provvedendo inoltre a:
    a. monitorare l'ambito dei trattamenti loro consentiti, nonché le banche dati e gli archivi cui hanno accesso, verificandone annualmente i presupposti e limiti, e segnalando all'UOC Risorse Umane e alla UOC Informatica eventuali cambiamenti per procedere all'aggiornamento periodico del relativo elenco;
    b. vigilare sull'osservanza, da parte delle persone Autorizzate, delle istruzioni impartite per il trattamento dei dati personali e delle vigenti disposizioni normative in materia di protezione dei dati personali, assicurando il rispetto dell'obbligo di riservatezza dei dati personali trattati e delle prassi aziendali in materia di trasmissione interna dei dati e di loro comunicazione all'esterno;

c. rendere disponibile (in formato elettronico o cartaceo), a ciascun Autorizzato del trattamento, il Regolamento privacy aziendale, adottando un sistema di distribuzione che garantisca l'effettiva conoscibilità del contenuti;

i. assicurare, per quanto di competenza, la corretta custodia e controllo, da parte delle persone Autorizzate al trattamento, dei documenti e degli strumenti elettronici ad essi affidati, in conformità con quanto previsto dai regolamenti e prassi aziendali;
j. assicurare la partecipazione del personale afferente alla propria UOC/UOSD ai percorsi formativi in materia di protezione dei dati personali promossi dal Titoalre del Trattamento;
k. segnalare all'UOC Affari Generali e Legali eventuali esigenze relative ad interventi di formazione e sensibilizzazione delle persone autorizzate al trattamento rispetto all'applicazione delle norme in materia di protezione dei dati personali e, ove necessario, fornire la necessaria collaborazione nella relativa programmazione e pianificazione;
l. gestire, nei limiti dei poteri conferiti e in collaborazione con le altre UOC competenti, i rapporti con i soggetti terzi che comportino operazioni di trattamento di dati personali, avendo cura di:
    a. definire i profili di reciproca responsabilità per detti rapporti attraverso l'utilizzo di contratti o clausole contrattuali definite in base agli standard aziendali per l'attribuzione ai terzi del ruolo di Responsabili esterni del trattamento di dati personali derivanti dalle attività ad essi affidate dal Titolare per conto e sotto il controllo di quest'ultimo;
    b. collaborare, ove richiesto, alla vigilanza sul loro operato ed osservanza delle istruzioni impartite in materia di protezione dei dati personali, secondo le prassi e procedure aziendali;
m. assicurare il rispetto delle condizioni previste dal GDPR per l'eventuale trasferimento di dati all'estero, verso cioè soggetti terzi stabiliti in Paesi Terzi al di fuori della UE, con conseguente applicazione delle adeguate garanzie a tutela degli interessati;
n. provvedere alla raccolta delle informazioni ed alle altre attività necessarie, in collaborazione con la UOC Affari Generali e Legali e il Responsabile della Protezione dei dati (RPD), per il riscontro alle richieste di esercizio dei diritti avanzate dagli interessati, nonché in relazione ad eventuali reclami e a richieste di informazioni od accertamenti dell'Autorità;
o. garantire la piena collaborazione della propria struttura in sede di effettuazione delle verifiche periodiche, effettuate dal Titolare tramite le apposite UOC deputate allo scopo, oltre al Responsabile per la protezione dei dati (RPD), aventi ad oggetto il rispetto delle

disposizioni ed istruzioni impartite in materia di privacy, anche per quanto attiene al rispetto delle misure di sicurezza.

Al Delegato Privacy (Responsabile del sistema informativo), quale responsabile della sicurezza del sistema informativo automatizzato aziendale si affidano, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa , delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti stabiliti per legge, ulteriori e specifici compiti di seguito elencati:

a. collabora con il Referente aziendale privacy e il Responsabile per la Protezione dei dati (RPD) nell'assolvimento delle funzioni per gli aspetti di propria competenza;
b. predispone e cura l'attuazione di quanto necessario in merito agli aspetti della sicurezza informatica dei trattamenti con strumenti elettronici;
c. cura i rapporti con il soggetto al quale l'Azienda ha affidato la gestione delle reti informative e delle tecnologie informatiche, al fine di garantire che le procedure informatiche siano conformi alla normativa in materia di protezione dei dati personali;
d. cura la tenuta dell'elenco delle banche dati informatiche custodite dall'Azienda, con indicazione delle rispettive sedi e caratteristiche;
e. cura la tenuta dell'elenco dei soggetti abilitati a ciascun applicativo secondo i profili di autorizzazione istituiti;
f. cura la tenuta e l'aggiornamento del "Registro elettronico delle attività di trattamento"; registro che sarà esibito dal Titolare (Direttore Generale dell'Azienda) su richiesta del Responsabile della Protezione dei Dati (RPD) aziendale e/o dell'Autorità Garante della privacy, come previsto dalla normativa vigente;
g. rimane a disposizione di Azienda Zero per fornire alla medesima azienda, quale ente di governance della sanità veneta, il contenuto del Registro delle attività di trattamento, ai fini di ottemperare agli sviluppi di carattere tecnologico ed organizzativo che Azienda Zero riterrà di porre in essere nell'ambito della rete regionale di cui fanno parte tutte le aziende sanitarie e ospedaliere del veneto;
h. redige, in collaborazione con le altre strutture all'uopo identificate per concorrere all'attuazione del documento, e tenendo conto dei principi esposti nelle linee guida metodologiche di Azienda Zero, trasmesse con nota prot. 16336 del 17/12/2018, la procedura aziendale relativa al Data Protection Impact Assessment (DPIA);
i. redige, in collaborazione con le altre strutture, all'uopo identificate per concorrere all'attuazione del documento, e tenendo conto dei principi esposti nelle linee guida metodologiche di Azienda Zero, la procedura di notifica al Garante delle violazioni dei dati personali nei casi previsti dal Regolamento UE (c.d. "Data Breach");

J. adotta, in collaborazione con le altre strutture, all'uopo identificate per concorrere all'attuazione del documento, e tenendo conto dei principi esposti nelle linee guida metodologiche di Azienda Zero, trasmesse con nota prot 16336 del 17/12/2018, le istruzioni operative per garantire i nuovi principi di "privacy by design" e "privacy by default" nell'intero ambito aziendale (Cioè in tutte le operazioni di trattamento dati, sia nella progettazione, che nella impostazione predefinita).

La delega conferita ai sopra individuati Delegati Privacy, è condizionata alla durata dell'incarico e si intende revocata di diritto alla cessazione dell'incarico medesimo, fermo restando in ogni caso la facoltà del Direttore Generale, in qualità di Titolare del trattamento dei dati, di ritirarla in caso di inadempimento dei compiti assegnati avocando pertanto a sé le relative funzioni;
Al fine di conferire continuità delle suddette responsabilità, la delega si estende ai dirigenti che, nel possibile periodo di vacanza del ruolo di Direttori di Struttura Complessa e di Responsabili di Struttura Semplice Dipartimentale e Responsabile dei sistemi informativi, assumano la relativa qualifica di facenti funzioni.

Tutto ciò premesso,

IL DIRETTORE GENERALE

PRESO ATTO della suestesa proposta e accertato che il Sostituto Responsabile della **UOC Affari Generali e Legali** ha attestato l'avvenuta regolare istruttoria della pratica, anche in ordine alla conformità con la vigente legislazione statale e regionale, nonché la copertura della spesa prevista nel budget assegnato per l'anno in corso;
RITENUTO di dover adottare in merito i provvedimenti necessari;
VISTO il Decreto Legislativo n. 502/92 e successive modifiche ed integrazioni e le leggi regionali n. 55 e n. 56 del 1994 e successive modifiche ed integrazioni;
ACQUISITO il parere favorevole del Direttore Amministrativo e del Direttore Sanitario per quanto di rispettiva competenza;
IN BASE ai poteri conferitigli dal D.P.G.R.nr.92 del 01.08.2016.

DELIBERA

1. di designare, a seguito della ridefinizione, per le ragioni espresse in premessa, dei profili di responsabilità in tema di protezione dei dati personali, i Direttori/Responsabili di UOC/UOSD quali Delegati al trattamento dei dati personali (**Delegati Privacy**) conferendo loro, ai sensi dell'art. 2- quaterdecies, comma 1 del novellato D.Lgs 196/2003, la delega relativa all'esercizio di funzioni di direzione,

coordinamento e controllo delle attività di trattamento dei dati personali, svolte nell'ambito delle attività di competenza della propria UOC/UOSD e dei correlati adempimenti previsti dal GDPR effettuati in tale ambito, affidando loro i compiti e le responsabilità, così come individuati in premessa;

2. di designare, altresì, quale Delegato al trattamento dei dati personali il Responsabile del sistema informativo, conferendogli con la delega relativa alla sicurezza del sistema informativo automatizzato aziendale, ulteriori e specifici compiti e responsabilità, così come individuati in premessa (**Delegato Privacy del sistema informativo automatizzato**);
3. di incaricare la UOC Risorse Umane di provvedere, dall'adozione del presente Atto, ad inserire nel contratto di lavoro, avente ad oggetto il conferimento di incarico dirigenziale di Unità Operativa Complessa e di Unità Operativa Semplice Dipartimentale, figure di cui al punto 1) e 2), la nomina di "Delegato Privacy" e a consegnare all'atto della sottoscrizione del contratto stesso la delega al trattamento dei dati personali di cui il dipendente prenderà atto sottoscrivendo per ricevuta;
4. di prevedere che per coloro che, alla data di adozione del presente provvedimento, ricoprono già l'incarico di Direttore/Responsabile di UOC/UOSD di cui ai punti 1) e 2), l'individuazione quale Delegato Privacy s'intende formalizzata con apposita comunicazione, a cura della UOC Affari Generali e Legali;
5. di ritenere che tale delega si esplichi in particolare nello svolgimento dei compiti citati in premessa, la cui elencazione non può comunque ritenersi esauriente rispetto a tutti i compiti e gli adempimenti connessi ad una compiuta e corretta attività di protezione dei dati, come in premessa specificati;
6. di dichiarare che la delega è condizionata alla durata dell'incarico e si intende revocata di diritto alla cessazione dell'incarico medesimo, fermo restando in ogni caso la facoltà del Direttore Generale, in qualità di Titolare del trattamento dei dati, di ritirarla in caso di inadempimento dei compiti assegnati avocando pertanto a sé le relative funzioni;
7. di specificare che, al fine di conferire continuità delle suddette responsabilità, la delega si estende ai dirigenti che, nel possibile periodo di vacanza del ruolo di Direttori di Struttura Complessa e di Responsabili di Struttura Semplice Dipartimentale, assumano la relativa qualifica di facenti funzioni;
8. di disporre che i Delegati Privacy rispondono al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla vigente normativa in materia di privacy e dalle istruzioni ricevute, ivi comprese quelle riguardanti l'adozione delle misure di sicurezza;

9. di designare quali **Autorizzati** al trattamento dei dati personali (ex incaricati), ai sensi degli artt. 4 n. 10, art. 29 e 32 comma 4 del GDPR, tutte le persone fisiche che a vario titolo svolgono attività all'interno delle varie strutture operative aziendali: dipendenti, sia a tempo indeterminato che determinato, personale universitario in convenzione, specialisti ambulatoriali interni, titolari di incarico libero professionali, di borse di studio, di collaborazioni occasionali, di co.co.co, di contratto di prestazione d'opera, frequentatori, tirocinanti e frequenze extra rete formativa e volontari;
10. di disporre che agli Autorizzati, di cui al punto precedente, vengano fornite, a cura del Delegato Privacy, Direttore di Unità Operativa Complessa o Responsabile di Unità Operativa Semplice Dipartimentale, alla quale gli Autorizzati sono stati formalmente assegnati, le **istruzioni operative** che si allegano al presente provvedimento (**All.1**);
11. di disporre, altresì, che agli Autorizzati, che svolgono attività di trattamento dei dati all'interno delle Unità Operative che erogano prestazioni sanitarie di pevenzione diagnosi cura e riabilitazione, vengano fornite, a cura del Delegato Privacy, Direttore di Unità Operativa Complessa o Responsabile di Unità Operativa Semplice Dipartimentale, alla quale gli stessi sono stati formalmente assegnati, le **ulteriori e specifiche istruzioni operative** che si allegano al presente provvedimento **(All.2)**;
12. di prevedere che venga impartita agli Autorizzati, a cura del Delegato Privacy, ogni altra istruzione scritta/verbale al fine di garantire il puntuale rispetto della normativa in materia di protezione dei dati personali;
13. di incaricare la UOC Risorse Umane, dall'adozione della presente deliberazione, di inserire nel contratto di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti) avente ad oggetto l'acquisizione del personale con funzioni diverse da quelle di direzione di Unità Operativa comprese le persone fisiche che a vario titolo dovranno svolgere temporaneamente la loro attività, una apposita clausola di designazione a " Autorizzato al trattamento dei dati personali" nonché il dovere del rispetto delle summenzionate istruzioni operative e di ogni altra istruzione scritta/verbale fornita e monitorata dal Delegato Privacy presso il quale la persona svolge la propria attività lavorativa;
14. di incaricare, altresì, la UOC Risorse Umane, nelle more della definizione di un sistema automatizzato, di comunicare, al Servizio Sistemi Informativi ogni spostamento interno, cessazione o altra variazione del predetto rapporto giuridico, che incida sulla figura di Autorizzato, per il blocco delle specifiche autorizzazioni precedentemente rilasciate per il trattamento dei dati;

15. di stabilire per coloro che, alla data di entrata in vigore del presente Regolamento, risultano avere già in atto un rapporto giuridico con l'Azienda, l'individuazione, quale Autorizzato al trattamento dei dati s'intende, formalizzata, nelle more della definizione di un sistema automatizzato, con la pubblicazione della presente delibera nel sito web aziendale nell'apposita sezione intranet ed internet, al fine di darne massima conoscibilità a tutti gli operatori aziendali;
16. di comunicare, con successivi specifici atti nominativi, prodotti da un sistema informatizzato in fase di definizione, l'esatto ambito di trattamento consentito dei dati, legato al profilo professionale a tutti i dipendenti/collaboratori dell'Azienda (Autorizzati al trattamento), di cui al punto 9);
17. di dare atto che al fine di presidiare il "sistema privacy", aziendale il nuovo assetto organizzativo interno è articolato su diversi livelli di responsabilità, così come riportato nelle premesse, che garantisce un "organigramma" funzionale alla messa a regime dell'auspicata piena realizzazione del dettato normativo e volta ad infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti i trattamenti, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero asset organizzativo, con particolare attenzione alle categorie particolari di dati, tra i quali quelli relativi alla salute;
18. di incaricare la UOC Affari Generali e Legali, con il supporto della UOC Rapporti con l'Università e Formazione,tenedo anche conto delle esigenze delle UOC/UOSD, di mettere in atto percorsi formativi in materia di protezione dei dati personali, per tutte le persone fisiche che a vario titolo svolgono attività all'interno delle Unità Operative aziendali (dipendenti, sia a tempo indeterminato che determinato, personale universitario in convenzione, specialisti ambulatoriali interni, titolari di incarico libero professionali, di borse di studio, di collaborazioni occasionali, di co.co.co, di contratto di prestazione d'opera, frequentatori, tirocinanti e frequenze extra rete formativa e volontari), che trattano dati nell'ambito dell'espletamento delle mansioni loro assegnate, al fine di sensibilizzare e favorire lo sviluppo di una cultura del rispetto della riservatezza e della protezione dei dati;
19. di ridefinire il percorso informativo anche attraverso l'implementazione di un'apposita area dedicata agli Autorizzati al trattamento dei dati personali, quale repository della documentazione aziendale sul tema, nella sezione privacy della intranet aziendale;
20. di dichiarare decaduti i precedenti provvedimenti non più compatibili con il nuovo assetto organizzativo;
21. di precisare, altresì, che qualora fosse necessario aggiornare l'assetto organizzativo, per renderlo rispondente alla normativa

tempo per tempo vigente, nonché ai Provvedimenti che l'Autorità Garante provvederà ad emanare e non ultimo alle modifiche del nuovo Atto Aziendale, ciò avverrà con semplice comunicazione interna all'Azienda, a prescindere dall'adozione di appositi atti deliberativi di modifica.

Il Direttore Generale
F.to Dott.Luciano Flor

ALLEGATO 1

AZIENDA OSPEDALIERA UNIVERSITA' PADOVA

Regione del Veneto
AZIENDA OSPEDALIERA – PADOVA

DIREZIONE GENERALE

ISTRUZIONI OPERATIVE

per gli Autorizzati al trattamento dei dati personali

(ex *artt. 4 n. 10, 29, 32 del Regolamento UE 2016/679 e dell'art. 2 quaterdecies comma 2 del D.Lgs 196/2003)*

In ottemperanza alle disposizioni del Regolamento UE 2016/679 per la protezione dei dati personali (nell'accezione inglese GDPR- *General Data Protection Regulation*) e al Decreto Legislativo 196/2003, novellato dal D.Lgs 101/2018, tutte le persone fisiche che a vario titolo prestano, anche temporaneamente, la loro attività all'interno delle varie strutture dell'Azienda Ospedaliera di Padova (dipendenti a tempo determinato e indeterminato, convenzionati con l'Università, specialisti ambulatoriali, interni, titolari di incarichi libero professionali, di borse di studio, di collaborazioni occasionali, di co.co.co, di contratto di prestazione d'opera, frequentatori, tirocinanti, frequenze extra rete, volontari) – designati dal Titolare quali "**Autorizzati al trattamento dei dati**" (art. 4, n. 10 del Regolamento UE 2016/679,)nello svolgimento delle operazioni di trattamento dei dati personali dovranno attenersi con scrupolo e diligenza alle **seguenti istruzioni** operative e ad ogni ulteriore indicazione, scritta e/o verbale, che potrà essere fornita dal Delegato Privacy (Direttore di UOC/Responsabile di UOSD) o dal Titolare stesso.

☐ **Trattamento di dati personali**

L'Art. 4 del GDPR 679/2016 definisce il trattamento di dati personali come "*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.*"

Il trattamento dev'essere:

a) effettuato secondo modalità tali da garantire la riservatezza;
b) effettuato in modo lecito e corretto e trasparente nei confronti dell'interessato;
c) raccolti per finalità determinate, esplicite e legittime;
d) realizzato in modo che non sia incompatibile con tali finalità;
e) limitato a quanto necessario rispetto alle finalità per le quali è stato raccolto;
f) deve avvenire 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 accidentale;
g) trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati.

☐ **Dato personale**

L'art. 4 del GDPR 2016/679 definisce "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**

L'art. 9 del GDPR 2016/679 definisce "dati particolari" *ogni Dato Personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*

☐ **Dati Giudiziari**

L'art. 10 del GDPR 2016/679 definisce "dati giudiziari" *indica ogni Dato Personale relativo a condanne penali e ai reati o a connesse misure di sicurezza ovvero relativo a provvedimenti giudiziari, sanzioni penali, o carichi pendenti, o la qualità dell'imputato o indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale.*

☐ **Obblighi formali**

Ogni soggetto autorizzato al trattamento dati è tenuto a:

- attuare le misure necessarie per un corretto, lecito, sicuro trattamento, attenendosi alle istruzioni operative ed alle prescrizioni definite nella regolamentazione aziendale (consultabile nel sito aziendale internet e intranet alla sezione privacy);
- accedere alle banche dati informatiche esclusivamente attraverso le proprie credenziali di autenticazione da tenere riservate
- richiedere l'autorizzazione al proprio Delegato Privacy per le modifiche e/o integrazioni del profilo autorizzativo che si rendessero necessarie;
- disporre quanto necessario a garantire la sicurezza delle modalità di trattamento di dati, sia digitali che cartacei, adottando adeguate misure contro accessi non autorizzati (*come ad esempio chiudere i locali dove sono conservati i dati, disconnettersi dalla propria postazione di lavoro)*;
- ottemperare agli obblighi di informazione e acquisizione del consenso;
- controllare e custodire, durante l'esecuzione del proprio lavoro, gli atti e i documenti contenenti dati, personali sensibili o giudiziari, in modo da impedirne l'accesso a persone non autorizzate;
- informare il proprio Delegato Privacy in merito alle eventuali richieste dell'interessato di esercitare i diritti previsti dagli artt. 12, 13 e 14 del GDRP 2016/679.

☐ **Accesso banche dati e Divieto di duplicazione banche dati**

L'accesso alle banche dati è limitato agli utilizzi previsti dalle mansioni attribuite al soggetto autorizzato. Non sono ammesse duplicazioni di data base contenenti dati personali, se non previa autorizzazione del Responsabile o Titolare.

☐ **Utilizzo e trasmissione dei dati**

Nel rispetto del principio di minimizzazione, i dati oggetto del trattamento possono essere utilizzati, condivisi, comunicati o inviati esclusivamente a persone che ne necessitano per lo svolgimento delle proprie mansioni lavorative e solo nel limite in cui i dati siano strettamente indispensabili.

I dati oggetto di trattamento non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (*anche se queste persone sono a loro volta soggetti autorizzati del trattamento*)

Nessun dato personale può essere utilizzato o trasmesso all'esterno senza previa autorizzazione del Delegato Privacy o del Titolare.

☐ **Strumenti informatici**

Al fine di garantire un corretto trattamento dei dati nel rispetto delle misure di sicurezza che l'Azienda ha ritenuto idoneo adottare, è opportuno impiegare gli strumenti elettronici ed informatici con diligenza ed attenzione, attenendosi alle disposizioni contenute nel "*Regolamento aziendale",* reso disponibile all'atto dell'assunzione e consultabile presso il sito aziendale: https://www.aopd.veneto.it/sez,82

A compendio di quanto indicato nel suddetto regolamento, sono comunque impartite queste direttive:

- Il trattamento di dati personali con strumenti elettronici è consentito alle figure dotati di credenziali di autenticazione (password riservata) che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti;
- I criteri di impostazione delle credenziali di autenticazione, così come la tempistica di cambiamento delle stesse, vengono comunicate dal Titolare del trattamento e/o del Delegato Privacy in relazione alla natura dei dati trattati e ai rischi sottesi a tali trattamenti;
- Non è consentito comunicare a nessuno le proprie password e soprattutto le stesse non vanno scritte su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata;
- Non è consentito lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- Non è consentito installare sulla propria postazione di lavoro programmi non attinenti alle normali attività d'ufficio né nuovi programmi necessari senza la preventiva autorizzazione del Titolare del trattamento e/o del proprio Delegato Privacy;
- Non è consentito modificare le configurazioni hardware e software senza 'autorizzazione del Titolare del trattamento e/o del proprio Delegato Privacy;
- Se si rileva un problema nell'ambito dell'utilizzo del sistema informatico relativo al trattamento di dati in corso che può compromettere la sicurezza dei dati (data breach) se ne dà immediata comunicazione al proprio Delegato Privacy che informa prontamente il Responsabile del sistema informativo;
- Accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il

mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati;
- Non è consentito scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti;
- Utilizzare la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali;
- Segnalare qualsiasi anomalia o stranezza di comportamento Tal proprio Delegato Privacy.

☐ **Credenziali**

Per il trattamento dei dati con gli strumenti elettronici in dotazione alla struttura il soggetto autorizzato viene dotato di credenziali di accesso (*username* e *password*).
Tali credenziali sono strettamente personali ed identificano l'operatore nella rete informatica.
Le caratteristiche e le norme da applicarsi a tutte le credenziali in uso al soggetto autorizzato, sono definite nel *Regolamento aziendale",* reso disponibile all'atto dell'assunzione e consultabile presso il sito aziendale: https://www.aopd.veneto.it/sez,82

☐ **Documenti cartacei**

I dati presenti su documenti cartacei devono essere tutelati mediante conservazione e gestione degli stessi in modo da evitarne la visibilità, la sottrazione, la riproduzione, l'alterazione o distruzione abusiva.

- I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento (*es. armadi o cassetti chiusi a chiave, uffici chiusi a chiave*).
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie stampanti, fotocopiatrici, fax o tavoli di lavoro.
- I documenti contenenti dati personali possono essere utilizzati, condivisi, comunicati o inviati esclusivamente a persone che ne necessitano per lo svolgimento delle proprie mansioni lavorative e solo nel limite in cui i dati siano strettamente indispensabili.

  I documenti contenenti dati personali non devono essere, condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (*anche se queste persone sono a loro volta soggetti autorizzati del trattamento*)
- Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili;
- I documenti che contengono dati sensibili e/o giudiziari devono essere controllati e custoditi dagli Autorizzati, i quali devono impedire l'accesso a persone prive di autorizzazione;
- L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

Il Direttore Generale
Dott. Luciano Flor
(Firmato digitalmente)

Presa visione

Il firmatario conferma di aver preso visione sia delle istruzioni operative dettagliate nei paragrafi precedenti, sia del regolamento citato nei paragrafi precedenti.

Data _____

Firma _____
(*destinatario della presente istruzione*)

ALLEGATO 2

Regione del Veneto
AZIENDA OSPEDALIERA – PADOVA
DIREZIONE GENERALE

ISTRUZIONI OPERATIVE ULTERIORI E SPECIFICHE

per gli Autorizzati che svolgono attività di trattamento dei dati all'interno delle Unità Operative che erogano prestazioni sanitarie di prevenzione diagnosi cura e riabilitazione

(ex *artt. 4 n. 10, 29, 32 del Regolamento UE 2016/679 e dell'art. 2 quaterdecies comma 2 del D.Lgs 196/2003 e s.m.i)*

Presso tutte le strutture di questa Azienda Ospedaliera che erogano prestazioni sanitarie gli Autorizzati devono garantire il rispetto della dignità e il massimo livello di tutela dei pazienti (provvedimento del Garante per la Protezione dei Dati Personali del 09/11/20005), osservando scrupolosamente le seguenti, ulteriori e specifiche istruzioni operative, sotto il diretto controllo del Delegato Privacy (Direttore/Responsabile UOC/UOSD):

- **Dignità dell'interessato.**

La tutela della dignità personale deve essere garantita nei confronti di tutti i soggetti cui viene erogata una prestazione sanitaria con particolare riguardo a fasce deboli quali disabili, fisici e psichici, minori e anziani, nonché - per effetto di specifici obblighi di legge o di regolamento – sieropositivi o affetti da infezione da Hiv, interruzione di gravidanza e persone offese da atti di violenza sessuale.
Nei reparti di rianimazione dove si possono visitare i degenti solo attraverso vetrate o videoterminali devono essere adottati accorgimenti, anche provvisori (ad esempio mediante paraventi), che delimitino le visibilità dell'interessato durante l'orario di visita ai soli familiari e conoscenti.
I Responsabili delle strutture dove, per finalità didattiche, alcune prestazioni sanitarie vengono erogate in presenza di studenti autorizzati, oltre ad informare preventivamente ogni singolo paziente di tale modalità, devono adottare specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie.

- **Riservatezza nei colloqui e nelle prestazioni sanitarie**.

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

- **Richiesta notizie su prestazioni di pronto soccorso.**

La notizia o la conferma di una prestazione di pronto soccorso, richieste anche per via telefonica, possono essere fornite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, valutate le diverse circostanze del caso. Il personale incaricato deve accertare l'identità dei terzi legittimati a ricevere la predetta notizia o conferma, avvalendosi anche di elementi desunti dall'interessato., valutate le diverse circostanze del caso, nella consapevolezza che si tratta di verifica dagli esiti incerti.
Le informazioni che possono essere fornite riguardano solo la circostanza che è in atto o si è svolta una prestazione di pronto soccorso e non anche informazioni più dettagliate sullo stato di salute dell'interessato.
L'interessato – se cosciente e capace – deve essere preventivamente informato (ad. es. in fase di accettazione) e posto in condizione di fornire indicazioni circa i soggetti che possono essere informati della prestazione di pronto soccorso. Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

- **Dislocazione dei pazienti nei reparti**.

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

Distanza di cortesia.

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

Ordine di precedenza e di chiamata.

Nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa (ad es. in caso di analisi cliniche) devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli interessati che prescinda dalla loro individuazione nominativa (ad es. attribuendo loro un codice numerico o alfanumerico fornito al momento della prenotazione o dell'accettazione). Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'interessato (ad es. nel caso di paziente disabile) possono essere utilizzati altri accorgimenti adeguati ed equivalenti come ad esempio il contatto diretto con il paziente.

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

Correlazione fra paziente e reparto o struttura.

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

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

Analoghe garanzie, infine, devono essere adottate nel caso di spedizione di plichi postali evitando che sugli stessi appaiano informazioni idonee a rivelare l'esistenza di uno stato di salute dell'interessato come l'indicazione della tipologia del contenuto del plico o del reparto mittente.

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

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

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

spedizione del referto tramite posta elettronica.

L'invio della copia del referto prodotto in formato digitale , alla casella di posta elettronica dell´interessato, a seguito di sua richiesta, deve osservare le seguenti cautele (Provvedimento dell'Autorità Garante del 19/11/2009 ad oggetto" *Linee guida in tema di referti on-line):*

1. spedizione del referto in forma di allegato a un messaggio *e-mail* e non come testo compreso nella *body part* del messaggio;
2. il file contenente il referto dovrà essere protetto con modalità idonee a impedire l´illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati, che potranno consistere in una *password* per l´apertura del file o in una chiave crittografica rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti Tale cautela può non essere osservata qualora l´interessato ne faccia espressa e consapevole richiesta, in quanto l´invio del referto alla casella di posta elettronica indicata dall´interessato non configura un trasferimento di dati sanitari tra diversi titolari del trattamento, bensì una comunicazione di dati tra la struttura sanitaria e l´interessato effettuata su specifica richiesta di quest´ultimo;
3. convalida degli indirizzi *e-mail* tramite apposita procedura di verifica *on-line*, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall´utente richiedente il servizio.

Il Direttore Generale
Dott. Luciano Flor
(firmato digitalmente)

Presa visione

Il firmatario conferma di aver preso visione delle istruzioni operative dettagliate nei paragrafi precedenti.

Data _____

Firma _____
(*destinatario della presente istruzione*)

ATTESTAZIONE DI PUBBLICAZIONE

La presente deliberazione e' stata pubblicata in copia all Albo di questa Azienda Ospedaliera di Padova per 15 giorni consecutivi dal

Il Sostituto Responsabile
UOC AFFARI GENERALI E LEGALI
(Avv.Maria Grazia Calì)

CERTIFICAZIONE DI ESECUTIVITA'

La presente deliberazione e' divenuta esecutiva il 7/3/2019

Il Sostituto Responsabile
UOC AFFARI GENERALI E LEGALI
(Avv.Maria Grazia Calì)

Copia composta di n°20 fogli (incluso il presente) della delibera n. 262 del 7/3/2019 firmata digitalmente dal Direttore Generale e conservata secondo la normativa vigente presso Infocert S.p.a.

Padova, li

Il Sostituto Responsabile
UOC AFFARI GENERALI E LEGALI
(Avv.Maria Grazia Calì)
