DETERMINA DEL DIRETTORE GENERALE AZIENDA SANITARIA TERRITORIALE DI PESARO E URBINO

n. 573 del 30 aprile 2024

Oggetto: Misure organizzative ex Regolamento UE 2016/679 (GDPR). Nomina "Designati" e "Autorizzati" al trattamento dei dati personali dell'Azienda Sanitaria Territoriale Pesaro Urbino

VISTO il documento istruttorio riportato in calce alla presente determina di cui costituisce parte integrante e sostanziale e dal quale si rileva la necessità di provvedere a quanto in oggetto specificato;

RITENUTO, per i motivi riportati nel predetto documento istruttorio, di adottare il presente atto;

ACQUISITI i pareri favorevoli del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio-Sanitario;

VISTE le attestazioni dei Direttori della UOC Affari Istituzionali e Generali, della UOC Controllo di Gestione e della UOC Bilancio, Patrimonio e Coordinamento Finanziamenti in riferimento alla spesa contenute nel "visto contabile";

DETERMINA

1. di nominare, ai sensi e per gli effetti di cui all'art.2 - *quaterdecies* del D.Lgs. 196/2003 e ss.mm.ii., quali soggetti "Designati" al trattamento dei dati personali dell'Azienda Sanitaria Territoriale Pesaro Urbino, i titolari dei seguenti incarichi presso l'Azienda stessa:
   - Direttori di Struttura Complessa (ovvero Titolari di incarichi di "sostituzione" nei termini previsti dai CC.NN.LL delle Aree contrattuali di riferimento)
   - Responsabili di Struttura Semplice Dipartimentale
   - Responsabile del *Servizio Prevenzione e Protezione*;
2. di dare atto che, sulla base della previsione normativa di cui al punto 1 del dispositivo, ai professionisti "Designati" vengono assegnati – in ragione del proprio ruolo di responsabilità organizzativa all'interno dell'Azienda – specifici compiti e funzioni di vigilanza sul rispetto e attuazione delle disposizioni in tema di trattamento di dati personali all'interno delle strutture rispettivamente dirette;
3. di dare, altresì atto che, in caso di vacanza degli incarichi di cui al punto 1 del dispositivo e nelle more del relativo conferimento, le correlate responsabilità in tema di protezione dei dati personali sono in capo al Direttore del Dipartimento, ove presente, ovvero al Direttore Sanitario e al Direttore Amministrativo a seconda dello specifico ambito organizzativo;
4. di trasmettere il presente atto a ciascun "Designato" al trattamento dei dati personali, unitamente alle relative istruzioni fornite dal Titolare cui i "Designati" medesimi sono tenuti ad attenersi nell'effettuare le attività di trattamento rientranti nelle rispettive funzioni istituzionali e che si allegano alla presente determina (All. n.1);
5. di dare atto che – in linea con le previsioni di cui agli artt. 4 n.10) e 29 del GDPR – tutto il Personale in

servizio all'interno delle diverse Unità Operative aziendali è "Autorizzato" al trattamento dei dati personali nell'ambito dello svolgimento delle attività istituzionali presso le strutture di rispettiva afferenza; ciò sotto la diretta autorità e vigilanza da parte dei soggetti "Designati" al trattamento e attenendosi alle istruzioni allegate alla presente determina (All. n.2), fatte salve le responsabilità di natura personale correlate all'autonomia professionale di specifiche categorie di professionisti;

6. di approvare - ad integrazione dei contenuti delle istruzioni di cui ai precedenti punti 4 e 5 del dispositivo – istruzioni specifiche per il trattamento dati da parte del personale sanitario, destinate sia ai "Designati" che a tutti gli "Autorizzati" al trattamento, che si allegano alla presente determina (All. n.3);
7. di dare mandato alle Strutture competenti in materia di gestione delle risorse umane di provvedere tempestivamente a formale comunicazione al RPD in ordine al vigente assetto degli incarichi di cui al precedente punto 1 del dispositivo - nonché a relativo aggiornamento - onde consentire allo stesso RPD l'espletamento di tutti gli incombenti in tema di protezione dei dati personali;
8. di dare mandato ai professionisti "Designati" al trattamento di produrre – secondo modalità da comunicarsi a cura del RPD - apposita attestazione comprovante l'avvenuta comunicazione dei contenuti del presente atto al Personale in servizio che effettua trattamenti di dati personali presso le Unità Operative rispettivamente dirette, ciò al fine di rendere edotti i medesimi in merito al contesto di riferimento ed alle richiamate specifiche istruzioni;
9. di dare mandato alle Strutture competenti in materia di gestione delle risorse umane di provvedere - in sede di conferimento di incarichi di direzione/responsabilità di struttura complessa ovvero di struttura semplice dipartimentale - all'inserimento di specifica clausola contrattuale ove il professionista venga nominato quale soggetto "Designato" al trattamento dei dati per la rispettiva Struttura, fornendo al medesimo le relative istruzioni di cui all'Allegato n.1 ed anche all'Allegato n.3 (solo per i professionisti sanitari);
10. di dare, altresì, mandato alle suddette Strutture competenti in materia di gestione delle risorse umane di provvedere - in sede di assunzione in servizio di nuove unità di Personale - all'inserimento di specifica clausola contrattuale contenente la nomina del neo assunto quale soggetto "Autorizzato" al trattamento, fornendo al medesimo le relative istruzioni di cui all'Allegato n.2 e anche all'Allegato n.3 (solo per i professionisti/operatori sanitari);
11. di dare mandato alla UOC Direzione Medica dei Presidi, alla UOC Direzione Amministrativa di Presidio e alla UOC Direzione Amministrativa Ospedaliera di provvedere - in sede di autorizzazione alla frequenza delle strutture aziendali da parte di volontari, tirocinanti, studenti e specializzandi - all'inserimento di specifica clausola contenente la nomina delle predette figure in qualità di "Autorizzati" al trattamento, fornendo loro le relative istruzioni di cui all'Allegato n.2 e anche all'Allegato n.3 (solo per i frequentatori di strutture/servizi sanitari);
12. di dare mandato alla UOC Gestione Amministrativa Personale Convenzionato e Strutture Accreditate di provvedere – in sede di reclutamento di personale convenzionato (Medici dell'Emergenza Sanitaria Territoriale, Medici Specialisti Ambulatoriali e Medici del Ruolo Unico di Assistenza Primaria a Rapporto Orario) - all'inserimento di specifica clausola contenente la nomina dei predetti professionisti in qualità di "Autorizzati" al trattamento, fornendo loro le relative istruzioni di cui all'Allegato n.2 e all'Allegato n.3;
13. di dare, altresì, atto che il Direttore della UOC Servizio Informatico, il Responsabile della UOC Sistemi Informativi Aziendali e il Responsabile della UOC Ingegneria Clinica ed *Information and Communication*

Tecnhology rivestono in Azienda anche il ruolo di "Amministratore di Sistema" relativamente alla funzionalità di tutti i sistemi/dispositivi informatici rientranti tra le attività di propria competenza, i quali provvedono conseguentemente alla designazione di Referenti – a loro supporto - dedicati a specifici ambiti di operatività all'interno delle Strutture di rispettiva afferenza, ciò secondo le apposite indicazioni fornite sul punto dall'Autorità Garante per la protezione dei dati con Provvedimento del 27.11.2008;

14. di dare atto che, a norma dell'art. 39, comma 8, della L.R. 19/2022 e ss.mm.ii., la presente determina è efficace dalla data di pubblicazione nell'all'Albo on line;
15. di trasmettere il presente atto al Collegio Sindacale per le valutazioni di competenza *ex* art.3-*ter* del D.Lgs. 502/1992 e ss.mm.ii..

Il Direttore Generale
(Dr.ssa Nadia Storti)

per i pareri infrascritti

Il Direttore Amministrativo	Il Direttore Sanitario	Il Direttore Socio-Sanitario
(Dott. Matteo Birasch	*(Dr. Edoardo Berselli)*	*(Dr. Nazzareno Firmani)*

Documento informatico firmato digitalmente

DOCUMENTO ISTRUTTORIO
UOC Affari Istituzionali e Generali

Normativa e atti di riferimento:

- **Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 (GDPR)** "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*";
- **Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii.** "*Codice in materia di protezione dei dati personali" (aggiornato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101);*
- **Legge Regionale 08 agosto 2022, n. 19** *"Organizzazione del Servizio Sanitario Regionale";*
- **DGRM n. 1718 del 19.12.2022** *"Adempimenti funzionali previsti dagli art. 42 e 43 della L.R. 8 agosto 2022, n. 19 (Organizzazione del servizio sanitario regionale) e DGRM 1385/2022*".

Con Legge regionale 8 agosto 2022, n. 19, ad oggetto "*Organizzazione del servizio sanitario regionale*", è stata soppressa, al 31 dicembre 2022, l'Azienda Sanitaria Unica Regionale (ASUR) e dal 1° gennaio 2023 sono state costituite e diventate operative le Aziende Sanitarie Territoriali, che sono subentrate all'ASUR senza soluzione di continuità.
Dal 1° gennaio 2023 - con la costituzione dell'Azienda Sanitaria Territoriale Pesaro Urbino - l'Azienda Ospedaliera Ospedali Riuniti Marche Nord è stata incorporata nella medesima Azienda Sanitaria Territoriale, che è subentrata a tutti gli effetti e senza soluzione di continuità nell'attività e nei rapporti giuridici attivi e passivi dell'Azienda Ospedaliera cessata.
Per quanto concerne la protezione dei dati personali trattati, l'Azienda Sanitaria Territoriale di Pesaro-Urbino, quale Titolare del trattamento ex art. 4 n.7) del Regolamento UE 2016/679 (GDPR), è tenuta – nella logica della piena applicazione del principio di *accountability* di cui all'art. 24 del GDPR stesso – a mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che i trattamenti di dati personali siano effettuati conformemente ai principi di cui al citato Regolamento UE.
Con specifico riferimento all'ambito delle misure organizzative da adottare, stante l'attuale fase di ristrutturazione del proprio l'assetto, questa AST necessita comunque di implementare una nuova architettura del sistema privacy, quale primo modello organizzativo in grado di continuare ad assicurare, anche in linea e continuità con i precedenti contesti, la più efficace applicabilità delle disposizioni normative in materia di protezione dei dati; ciò nelle more di addivenire alla completa definizione e realizzazione del predetto processo di riorganizzazione a seguito dell'adozione dell'Atto aziendale.
Pertanto, il Titolare del trattamento - in ragione della complessità ed eterogeneità delle funzioni in capo all'Azienda, dell'esigenza di rendere tempestiva ed efficace la vigilanza sui trattamenti e sulla protezione dei dati a livello di tutte le Unità Operative che la costituiscono e nell'ottica di presidiare il sistema privacy mediante una strutturazione interna articolata sui diversi livelli di responsabilità - ritiene, in conformità al vigente quadro

normativo di riferimento, di nominare quali soggetti "Designati" al trattamento dei dati personali i titolari, presso l'Azienda stessa, dei seguenti incarichi:

- Direttori di Struttura Complessa (ovvero Titolari di incarichi di "sostituzione" nei termini previsti dai CC.NN.LL delle Aree contrattuali di riferimento)
- Responsabili di Struttura Semplice Dipartimentale
- Responsabile del Servizio Prevenzione e Protezione.

Conseguentemente ed in coerenza con le disposizioni di cui alla DGRM n.1718/2022, le citate designazioni sono riconducibili agli incarichi in essere di direzione/responsabilità delle Strutture/Servizi afferenti ai distinti ambiti organizzativi e funzionali, rispettivamente, dell'ex Azienda Ospedaliera Ospedali Riuniti Marche Nord e dell'ex ASUR - Area Vasta 1.

E' opportuno evidenziare che ai professionisti "Designati" al trattamento dei dati personali vengono assegnati da parte del Titolare - in ragione del proprio ruolo di responsabilità organizzativa all'interno dell'Azienda – specifici compiti e funzioni volti ad assicurare la corretta applicazione delle disposizioni in materia di protezione dei dati personali nell'ambito delle strutture rispettivamente dirette, sulla base di specifiche istruzioni fornite dal Titolare stesso e in coerenza con il quadro disciplinare di cui all'art. 2–*quaterdecies* del D.Lgs. 196/2003 e ss.mm.ii., il quale contempla che:

"*1. Il titolare o il responsabile possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*".

Sempre in linea con il quadro normativo vigente in materia, ovvero con le previsioni di cui agli artt. 4 n.10) e 29 del GDPR, tutto il Personale a vario titolo in servizio all'interno delle diverse Unità Operative aziendali è "Autorizzato" al trattamento dei dati personali nell'ambito dello svolgimento delle attività istituzionali presso le strutture di rispettiva afferenza; ciò sotto la diretta autorità e vigilanza da parte dei soggetti "Designati" al trattamento, attenendosi alle istruzioni date ed in conformità all'art. 32, comma 4, del GDPR il quale, appunto, prevede che il Titolare del trattamento fa si che chiunque agisca sotto la sua autorità e abbia accesso a dati personali non li tratti se non è in tal senso istruito dal Titolare medesimo.

Il Direttore della UOC Servizio Informatico, il Responsabile della UOC Sistemi Informativi Aziendali e il Responsabile della UOC Ingegneria Clinica ed *Information and Communication Tecnhology* – oltre ad essere soggetti "Designati" al trattamento dei dati personali dell'Azienda – rivestono presso l'Azienda stessa anche il ruolo di "Amministratori di Sistema" relativamente alla funzionalità di tutti i sistemi/dispositivi informatici rientranti tra le attività di propria competenza, i quali provvedono conseguentemente alla individuazione di Referenti, a loro supporto, dedicati a specifici ambiti di operatività all'interno delle Strutture di rispettiva afferenza; ciò secondo le apposite indicazioni fornite sul punto dall'Autorità Garante per la protezione dei dati con Provvedimento del 27.11.2008.

Per quanto sopra esposto, si propone al Direttore Generale il seguente schema di dispositivo:

1. di nominare, ai sensi e per gli effetti di cui all'art.2 - *quaterdecies* del D.Lgs. 196/2003 e ss.mm.ii., quali soggetti "Designati" al trattamento dei dati personali dell'Azienda Sanitaria Territoriale Pesaro Urbino, i titolari dei seguenti incarichi presso l'Azienda stessa:
   - Direttori di Struttura Complessa (ovvero Titolari di incarichi di "sostituzione" nei termini previsti dai CC.NN.LL delle Aree contrattuali di riferimento)
   - Responsabili di Struttura Semplice Dipartimentale
   - Responsabile del *Servizio Prevenzione e Protezione*;
2. di dare atto che, sulla base della previsione normativa di cui al punto 1 del dispositivo, ai professionisti "Designati" vengono assegnati – in ragione del proprio ruolo di responsabilità organizzativa all'interno dell'Azienda – specifici compiti e funzioni di vigilanza sul rispetto e attuazione delle disposizioni in tema di trattamento di dati personali all'interno delle strutture rispettivamente dirette;
3. di dare, altresì atto che, in caso di vacanza degli incarichi di cui al punto 1 del dispositivo e nelle more del relativo conferimento, le correlate responsabilità in tema di protezione dei dati personali sono in capo al Direttore del Dipartimento, ove presente, ovvero al Direttore Sanitario e al Direttore Amministrativo a seconda dello specifico ambito organizzativo;
4. di trasmettere il presente atto a ciascun "Designato" al trattamento dei dati personali, unitamente alle relative istruzioni fornite dal Titolare cui i "Designati" medesimi sono tenuti ad attenersi nell'effettuare le attività di trattamento rientranti nelle rispettive funzioni istituzionali e che si allegano alla presente determina (All. n.1);
5. di dare atto che – in linea con le previsioni di cui agli artt. 4 n.10) e 29 del GDPR – tutto il Personale in servizio all'interno delle diverse Unità Operative aziendali è "Autorizzato" al trattamento dei dati personali nell'ambito dello svolgimento delle attività istituzionali presso le strutture di rispettiva afferenza; ciò sotto la diretta autorità e vigilanza da parte dei soggetti "Designati" al trattamento e attenendosi alle istruzioni allegate alla presente determina (All. n.2), fatte salve le responsabilità di natura personale correlate all'autonomia professionale di specifiche categorie di professionisti;
6. di approvare - ad integrazione dei contenuti delle istruzioni di cui ai precedenti punti 4 e 5 del dispositivo – istruzioni specifiche per il trattamento dati da parte del personale sanitario, destinate sia ai "Designati" che a tutti gli "Autorizzati" al trattamento, che si allegano alla presente determina (All. n.3);
7. di dare mandato alle Strutture competenti in materia di gestione delle risorse umane di provvedere tempestivamente a formale comunicazione al RPD in ordine al vigente assetto degli incarichi di cui al precedente punto 1 del dispositivo - nonché a relativo aggiornamento - onde consentire allo stesso RPD l'espletamento di tutti gli incombenti in tema di protezione dei dati personali;
8. di dare mandato ai professionisti "Designati" al trattamento di produrre – secondo modalità da comunicarsi a cura del RPD - apposita attestazione comprovante l'avvenuta comunicazione dei contenuti del presente atto al Personale in servizio che effettua trattamenti di dati personali presso le Unità Operative rispettivamente dirette, ciò al fine di rendere edotti i medesimi in merito al contesto di riferimento ed alle richiamate specifiche istruzioni;
9. di dare mandato alle Strutture competenti in materia di gestione delle risorse umane di provvedere - in sede di conferimento di incarichi di direzione/responsabilità di struttura complessa ovvero di struttura semplice dipartimentale - all'inserimento di specifica clausola contrattuale ove il professionista venga nominato quale

soggetto "Designato" al trattamento dei dati per la rispettiva Struttura, fornendo al medesimo le relative istruzioni di cui all'Allegato n.1 ed anche all'Allegato n.3 (solo per i professionisti sanitari);

10. di dare, altresì, mandato alle suddette Strutture competenti in materia di gestione delle risorse umane di provvedere - in sede di assunzione in servizio di nuove unità di Personale - all'inserimento di specifica clausola contrattuale contenente la nomina del neo assunto quale soggetto "Autorizzato" al trattamento, fornendo al medesimo le relative istruzioni di cui all'Allegato n.2 e anche all'Allegato n.3 (solo per i professionisti/operatori sanitari);
11. di dare mandato alla UOC Direzione Medica dei Presidi, alla UOC Direzione Amministrativa di Presidio e alla UOC Direzione Amministrativa Ospedaliera di provvedere - in sede di autorizzazione alla frequenza delle strutture aziendali da parte di volontari, tirocinanti, studenti e specializzandi - all'inserimento di specifica clausola contenente la nomina delle predette figure in qualità di "Autorizzati" al trattamento, fornendo loro le relative istruzioni di cui all'Allegato n.2 e anche all'Allegato n.3 (solo per i frequentatori di strutture/servizi sanitari);
12. di dare mandato alla UOC Gestione Amministrativa Personale Convenzionato e Strutture Accreditate di provvedere – in sede di reclutamento di personale convenzionato (Medici dell'Emergenza Sanitaria Territoriale, Medici Specialisti Ambulatoriali e Medici del Ruolo Unico di Assistenza Primaria a Rapporto Orario) - all'inserimento di specifica clausola contenente la nomina dei predetti professionisti in qualità di "Autorizzati" al trattamento, fornendo loro le relative istruzioni di cui all'Allegato n.2 e all'Allegato n.3;
13. di dare, altresì, atto che il Direttore della UOC Servizio Informatico, il Responsabile della UOC Sistemi Informativi Aziendali e il Responsabile della UOC Ingegneria Clinica ed *Information and Communication Tecnhology* rivestono in Azienda anche il ruolo di "Amministratore di Sistema" relativamente alla funzionalità di tutti i sistemi/dispositivi informatici rientranti tra le attività di propria competenza, i quali provvedono conseguentemente alla designazione di Referenti – a loro supporto - dedicati a specifici ambiti di operatività all'interno delle Strutture di rispettiva afferenza, ciò secondo le apposite indicazioni fornite sul punto dall'Autorità Garante per la protezione dei dati con Provvedimento del 27.11.2008;
14. di dare atto che, a norma dell'art. 39, comma 8, della L.R. 19/2022 e ss.mm.ii., la presente determina è efficace dalla data di pubblicazione nell'all'Albo on line;
15. di trasmettere il presente atto al Collegio Sindacale per le valutazioni di competenza *ex* art.3-*ter* del D.Lgs. 502/1992 e ss.mm.ii..

Si richiede la pubblicazione all'*Albo on line*:

[x] INTEGRALE

Il Direttore
(Dott.ssa Emanuela Raho)

Il Responsabile della protezione dei dati
(Dott.ssa Federica Pierleoni)

Documento informatico firmato digitalmente

ALLEGATI

La presente determina contiene i seguenti allegati:

- All. n.1 – Istruzioni ai "Designati" al trattamento dei dati personali
- All. n.2 – Istruzioni agli "Autorizzati" al trattamento dei dati personali
- All. n.3 – Istruzioni specifiche per il trattamento dati da parte di personale sanitario, destinate sia ai "Designati" che agli "Autorizzati" al trattamento

AZIENDA SANITARIA TERRITORIALE

Compiti e istruzioni ai professionisti "Designati" al trattamento dei dati personali nell'ambito dell'organizzazione dell'Azienda Sanitaria Territoriale di Pesaro - Urbino

PRINCIPI GENERALI

In conformità ai contenuti dell'art. 5 del Regolamento Europeo 2016/679 (GDPR) che prescrive i "*principi applicabili al trattamento dei dati personali*", il professionista "Designato" al trattamento dei dati personali è tenuto a garantire che ciascuna attività di trattamento dati - effettuata nell'ambito della struttura dallo stesso diretta - avvenga in osservanza dei seguenti principi di ordine generale:

- **liceità**, vale a dire nel rispetto delle Leggi, comprese quelle che regolano specifici settori;
- **correttezza**, vale a dire nel rispetto delle reciproche esigenze dell'Azienda e dell'Interessato, oltre agli obblighi derivanti dal quadro normativo;
- **trasparenza**, nel senso di assicurare la piena consapevolezza dell'Interessato, con particolare riferimento all'obbligo di rendere conoscibili all'utenza le modalità con cui i dati sono raccolti, utilizzati e consultati attraverso informazioni e comunicazioni facilmente accessibili, utilizzando un linguaggio semplice e chiaro.

I dati devono essere raccolti solo per **scopi**:

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

I dati devono, inoltre, essere:

- **esatti**, ossia, precisi e rispondenti al vero e, se necessario, **aggiornati**;
- **pertinenti**, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;

- **non eccedenti** in senso quantitativo rispetto allo scopo perseguito; ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine ed in mancanza dei quali non sia possibile il perseguimento del fine stesso;

- **conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle specifiche disposizioni di Legge cui è tenuto il Titolare. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione non è più consentita. In particolare, i dati idonei a rivelare lo **stato di salute** o la **vita sessuale devono** essere accuratamente conservati;

- **sicuri,** cioè deve essere garantita la sicurezza nel trattamento, compresa la protezione mediante misure tecniche e organizzative adeguate, atte a impedirne la perdita, distruzione o danno accidentale (integrità e riservatezza).

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dai principi fondamentali di **integrità, riservatezza** e **rispetto della dignità della persona fisica dell'interessato**, ovvero deve essere effettuato eliminando ogni rischio di impropria conoscibilità dei dati da parte di terzi e di perdita o distruzione del dato.

COMPITI SPECIFICI DEL "DESIGNATO" AL TRATTAMENTO

Il professionista "Designato" al trattamento dei dati personali - nell'ambito dello svolgimento delle attività istituzionali all'interno della struttura dallo stesso diretta comportanti operazioni di trattamento di dati personali - è tenuto a:

☐ trattare i dati personali osservando le vigenti disposizioni normative in materia di Privacy;

☐ vigilare che ogni soggetto "Autorizzato", nello svolgimento delle operazioni strettamente connesse all'adempimento delle proprie funzioni, si attenga scrupolosamente alle istruzioni impartite curando, in particolare, il profilo della riservatezza, della sicurezza di accesso e dell'integrità dei dati medesimi;

☐ adottare tutte le preventive misure di sicurezza ritenute idonee al fine di ridurre al minimo i rischi di distruzione, perdita e danno accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

☐ vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o ove vengono trattati dati sensibili o giudiziari;

☐ attenersi alle procedure aziendali relative alla gestione delle credenziali di autenticazione informatica per:
- l'attivazione di nuove profilazioni a fronte di nuove assunzioni o cambi mansione;
- la disattivazione delle credenziali di autenticazione informatica assegnate al personale "Autorizzato" per l'accesso ai singoli sistemi applicativi anche in caso di perdita della qualità che consente al soggetto "Autorizzato" l'accesso ai dati personali (ad esempio cambio mansioni o trasferimenti ad altra UO);

☐ adottare idonee misure finalizzate a garantire la dignità delle persone e la riservatezza dei dati trattati in relazione a richieste o fruizioni di prestazioni sanitarie, secondo le indicazioni e i processi aziendali anche di natura informatica;

☐ proporre al Titolare del trattamento – in caso di stipula di contratti pubblici finalizzati all'acquisizione di beni e servizi che implichino attività di trattamento dati - la nomina dei soggetti esterni all'Azienda in qualità di Responsabili del trattamento ai sensi dell'articolo 28 del GDPR;

☐ garantire al Titolare la piena collaborazione in sede di effettuazione delle verifiche periodiche aventi ad oggetto l'accertamento del rispetto delle istruzioni impartite, anche per quanto attiene il rispetto delle misure di sicurezza;

☐ utilizzare il PC, internet e la posta elettronica attenendosi alle indicazioni e prescrizioni fornite dalla UOC Servizio Informatico;

☐ collaborare con il Responsabile per la transizione al digitale - nell'ambito dell'attuazione del piano triennale Agid - alla costante revisione dei processi verso la digitalizzazione;

☐ collaborare con il Responsabile della protezione dei dati ai fini dell'implementazione e costante aggiornamento del Registro delle attività di trattamento;

☐ collaborare con il Responsabile della protezione dei dati - limitatamente all'ambito e agli aspetti di competenza – all'analisi dei rischi che incombono sui trattamenti di dati personali effettuati presso la struttura dallo stesso diretta;

☐ informare il Titolare e il Responsabile della protezione dei dati in merito ad ogni questione avente particolare rilevanza in termini di impatto sulla protezione dei dati;

☐ consultare preventivamente il Titolare e il Responsabile della protezione dei dati nell'eventualità di trasferimento di dati personali in Paesi non appartenenti all'Unione Europea.

AZIENDA SANITARIA TERRITORIALE

Istruzioni agli "Autorizzati" al trattamento dei dati personali all'interno dell'organizzazione dell'Azienda Sanitaria Territoriale di Pesaro - Urbino

PRINCIPI GENERALI

Al fine di una corretta applicazione dei principi e delle disposizioni contenute nel Regolamento Europeo 2016/679 (GDPR) in materia di protezione dei dati personali, il soggetto "Autorizzato" è tenuto – nell'ambito delle attività di trattamento effettuate presso la struttura di appartenenza sotto la diretta autorità e vigilanza del "Designato" al trattamento - ad osservare le seguenti istruzioni impartite dal "Designato" medesimo, ovvero:

☐ effettuare le operazioni di trattamento dei dati personali (ivi compresi i dati sensibili e giudiziari) strettamente necessarie allo svolgimento delle attività cui si è preposti nell'ambito della struttura di assegnazione;

☐ trattare tutti i dati personali di cui si viene a conoscenza nell'ambito dello svolgimento delle proprie funzioni secondo liceità e correttezza e, comunque, in modo tale da garantire, in ogni operazione di trattamento, la massima riservatezza;

☐ verificare che i dati trattati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati;

☐ accedere unicamente alle banche dati presenti presso la struttura in cui si presta la propria attività lavorativa;

☐ mantenere assoluto riserbo sui dati personali di cui si viene a conoscenza nell'esercizio delle proprie funzioni;

☐ evitare l'uso di strumenti informatici personali e del telefono cellulare per il trattamento di dati personali e sensibili acquisiti durante l'attività di servizio; ciò vale anche in caso di rilascio pareri e consulenze;

☐ utilizzare il PC, internet e la posta elettronica attenendosi alle indicazioni e prescrizioni fornite dalla UOC Servizio Informatico;

☐ attenersi alle disposizioni aziendali in tema di conservazione ed archiviazione dei dati e di accesso agli archivi locali e centralizzati di raccolta dei dati.

Il personale "Autorizzato" effettua le attività di trattamento dei dati nell'ambito della struttura di appartenenza sotto la diretta autorità e vigilanza del professionista "Designato" al trattamento, fatte salve le responsabilità di natura personale correlate all'autonomia professionale di specifiche categorie di professionisti.

PER I TRATTAMENTI EFFETTUATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

- I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave);

- I documenti contenenti dati personali prelevati ed estratti dagli archivi per lo svolgimento dell'attività quotidiana devono esservi riposti a fine giornata;

- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro. In caso di allontanamento - anche temporaneo - dal posto di lavoro, adottare le misure in atto a propria disposizione (secondo le istruzioni ricevute) per evitare l'accesso ai dati personali trattati o in trattamento, da parte di soggetti terzi, anche dipendenti, non autorizzati;

- 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 incaricate del trattamento);

- Qualora sia necessario eliminare documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere frammentati in maniera tale da non essere più ricomponibili;

- I documenti che contengono dati sensibili e/o giudiziari devono essere controllati e custoditi dagli "Autorizzati" al trattamento, 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.

PER I TRATTAMENTI EFFETTUATI CON L'AUSILIO DI STRUMENTI ELETTRONICI

- Il trattamento di dati personali con strumenti elettronici è consentito soltanto agli "Autorizzati" dotati di credenziali che permettano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'"Autorizzato" associato a una parola chiave riservata conosciuta solamente dal medesimo;

- La password deve essere modificata dall'"Autorizzato" almeno ogni 90 giorni solari;

- La password deve essere composta da almeno otto caratteri comprendenti lettere maiuscole e minuscole, numeri e caratteri speciali;

- Nel digitare la password accertarsi che non ci sia nessuno che osservi e sia in grado di vedere od intuire i caratteri digitati sulla tastiera;

- Aver cura di non scrivere le proprie password su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata;

- In presenza di ospiti occorre lasciare attendere questi ultimi in luoghi in cui non siano presenti informazioni riservate o dati personali;

- Non si deve lasciare incustodito e accessibile lo strumento elettronico (p.c.) durante una sessione di trattamento. In caso di allontanamento, anche temporaneo, dal posto di lavoro, occorre attivare adottare la procedura c.d. "salva schermo";

- Se nell'ambito dell'utilizzo del sistema informatico attraverso il quale viene effettuata attività di trattamento di dati si rileva una problematica tale da compromettere la sicurezza dei dati stessi, l'"Autorizzato" è tenuto a darne immediata comunicazione al professionista "Designato" al trattamento;

- Si deve accedere unicamente alle banche dati presenti presso l'Unità Organizzativa in cui si presta la propria attività lavorativa;

- Evitare di creare banche dati nuove senza espressa autorizzazione del Titolare o del designato in qualità di Responsabile "interno" del trattamento;

- È fatto assoluto divieto di comunicare o diffondere i dati personali provenienti da banche dati aziendali in assenza dell'autorizzazione del Titolare o del designato in qualità di Responsabile "interno" del trattamento;

- Accertarsi che sul proprio *personal computer* sia sempre operativo un programma antivirus, aggiornato e con la funzione di monitoraggio attiva;

- Sottoporre a controllo mediante il programma antivirus installato sul proprio *personal computer* tutti i supporti di provenienza esterna prima di eseguire *file* in essi contenuti;

- Non è consentito l'uso e l'installazione di *software* non aziendali senza l'autorizzazione della competente UOC Servizio Informatico;

- Assicurarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; in caso di dubbio procedere alla cancellazione del messaggio senza aprire gli allegati;

- La connessione ad Internet deve essere utilizzata esclusivamente per lo svolgimento dei propri compiti istituzionali;

- Informare il professionista "Designato" al trattamento in caso di incidenti di sicurezza o di eventuali anomalie che coinvolgono i dati personali all'interno della struttura di afferenza;

- Osservare tutte le misure tecniche, organizzative e di sicurezza adottate a livello aziendale, oltre le eventuali ulteriori istruzioni che verranno comunicate dal Titolare, dal "Designato" al trattamento o dal Responsabile della protezione dei dati.

AZIENDA SANITARIA TERRITORIALE

Istruzioni specifiche per il personale sanitario destinate sia ai "Designati" che agli "Autorizzati" al trattamento dei dati personali

Indice

PREMESSA

Le presenti istruzioni – specifiche per il personale sanitario che svolge la propria attività lavorativa in contesti, quali, l'ambito ospedaliero, ambulatori, distretti, strutture territoriali, ecc. - hanno lo scopo di chiarire e diffondere regole/misure comportamentali, organizzative e tecniche cui i professionisti "Designati" e gli "Autorizzati" al trattamento devono attenersi nello svolgimento delle operazioni di trattamento dei dati personali all'interno dell'organizzazione aziendale, al fine di ridurre e contenere i rischi di danneggiamento, dispersione o perdita di dati a causa di un uso non corretto o illecito dei sistemi informatici e degli archivi cartacei.

1. ISTRUZIONI GENERALI

1.1. - Segreto professionale o d'ufficio

I "Designati" e gli "Autorizzati" al trattamento sono tenuti a mantenere la necessaria riservatezza sulle informazioni di cui vengono a conoscenza nello svolgimento della propria attività lavorativa e professionale e nel corso delle operazioni di trattamento, evitando di comunicare informazioni e dati a terzi.

Tutto il personale del comparto e della dirigenza – appartenente al ruolo medico, sanitario, tecnico - e chiunque presti la propria attività lavorativa in ambito sanitario (anche in veste di consulente, libero/professionista, tirocinante, volontario, specializzando, personale convenzionato) presso le strutture dell'Azienda è tenuto al segreto professionale o al segreto d'ufficio, ossia a non rivelare e/o agevolare in qualsiasi modo, senza giusta causa, la conoscenza di notizie, dati o banche dati di cui - in ragione e in occasione del proprio stato o ufficio - sia venuto a conoscenza. L'eventuale violazione di tale obbligo può comportare l'applicazione di sanzioni di natura deontologica e disciplinare, nonché una responsabilità di natura amministrativa, civile e penale, secondo quanto previsto dalla legge.

1.2. - Tutela della dignità della persona

Deve essere sempre tutelata la dignità di tutti i soggetti che usufruiscono di prestazioni sanitarie, con particolare riguardo alle fasce deboli (ad es. disabili fisici o psichici, minori e anziani), pazienti sieropositivi o affetti da infezione da HIV, pazienti sottoposti a trattamenti medici invasivi, soggetti particolarmente vulnerabili (ad es. interruzione volontaria di gravidanza o vittime di atti di violenza sessuale o di genere).

Nelle terapie intensive o nei reparti che consentono la visione dei pazienti attraverso sistemi di videosorveglianza sanitaria devono essere utilizzati paraventi o altri accorgimenti che limitino la visibilità dell'interessato, durante l'orario di visita, ai soli familiari e conoscenti.

1.3. - Riservatezza nei colloqui e nel corso di prestazioni sanitarie

Durante i colloqui con l'interessato o con soggetti dallo stesso individuati, o durante l'esecuzione di prestazioni sanitarie, vanno adottate opportune cautele per evitare che le informazioni sulla salute possano essere conosciute da terzi. Analoghe cautele vanno adottate in occasione della raccolta di dati anamnestici, qualora ciò avvenga in situazioni di promiscuità.

Tutti i professionisti e operatori devono evitare di discutere sulle condizioni cliniche dei pazienti in pubblico, nei luoghi comuni (es. corridoi, bar, ascensore), in presenza di estranei o mediante o utilizzando altre modalità - quali social network, videoconferenza pubblica - ricorrendo a riferimenti che rendano direttamente o indirettamente identificabile la persona.

1.4. – Comunicazioni sulla presenza del Paziente in Ospedale

Utilizzando la modulistica appositamente predisposta, l'interessato – se cosciente e capace – all'atto del ricovero o dell'accesso in Pronto Soccorso deve essere informato e posto in condizione di fornire indicazioni circa i soggetti che possono ricevere notizie sul suo stato di salute e/o sulla sua presenza presso le diverse strutture dell'Azienda. Deve essere rispettata l'eventuale decisione dell'interessato di non rendere nota la sua presenza in ospedale.

1.5. - Comunicazione all'interessato o a terzi legittimati

La comunicazione al paziente di informazioni sul suo stato di salute deve essere effettuata solo da personale medico o da altro operatore sanitario che intrattenga rapporti diretti con il paziente (ad esempio personale infermieristico autorizzato dal responsabile della Struttura).

Le informazioni sullo stato di salute possono essere fornite a soggetti diversi dall'interessato solo se espressamente individuati dal medesimo, mediante la modulistica in uso, oppure nei casi previsti dalla legge.

Pertanto, prima di dare informazioni a terzi legittimati (ad esempio: coniuge, convivente, figli, genitori, fratelli, ecc.) occorre verificare che il paziente non abbia espresso volontà contraria o abbia identificato solo particolari soggetti destinatari dell'informazione, accertandosi - per quanto possibile - dell'identità dei soggetti richiedenti.

Nel caso di pazienti minori con genitori separati con affidamento esclusivo, la comunicazione di notizie al genitore non affidatario può avvenire solo previo consenso esplicito di quello affidatario.

Con specifico riferimento alle categorie particolari di dati personali, le notizie da fornire, specie se destinate a soggetti terzi (es. medico di famiglia), devono limitarsi ai soli elementi pertinenti e necessari per le finalità di cura.

1.6. – Rilascio notizie a mezzo telefono o ad organi di stampa

E' vietato fornire dati e informazioni di carattere sanitario tramite telefono ad eccezione dei pazienti e delle persone da questi autorizzate e solo se si abbia certezza assoluta dell'identità del chiamante.

Nel caso in cui giungano richieste telefoniche di dati sanitari da parte dell'Autorità Giudiziaria o degli organi di polizia occorre verificare preliminarmente l'identità del soggetto richiedente richiamando l'interlocutore al numero da questi comunicato.

È fatto divieto di comunicare dati personali o sanitari agli organi di stampa; le eventuali richieste di informazioni devono essere inoltrate alla Direzione Generale per il tramite dell'URP.

1.7. - Distanze di cortesia

Tutti i punti di accettazione e front office devono rispettare una distanza di cortesia, evidenziata da una striscia gialla di segnalazione posta a terra e da un avviso o cartello per l'utenza, sia per operazioni amministrative allo sportello (prenotazione, accettazione, ritiro referti), sia per l'acquisizione di dati personali comuni e relativi alla salute.

1.8. - Ordine di chiamata

Gli utenti in attesa di visita o di accertamenti (ad es. analisi cliniche o indagini di radiologia) non devono essere chiamati direttamente per nome o cognome ma mediante chiamata non nominativa (eliminacode, numero di prenotazione CUP o attribuzione di un codice numerico o alfanumerico al momento dell'accettazione).

1.9. - Liste di pazienti

E' vietata 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.

1.10. - Cartella clinica e documentazione sanitaria

In caso di trasferimento interno dei pazienti ricoverati tra i diversi Presidi o Strutture o nel caso di consulenza o accertamenti diagnostici, la documentazione sanitaria del paziente deve essere riposta in buste o raccoglitori chiusi e non trasparenti, in modo da non permettere la lettura dei dati sensibili da parte di personale non autorizzato.

La documentazione deve essere presa in custodia dal personale sanitario incaricato e da questi consegnata alla struttura di destinazione o restituita alla struttura di provenienza al termine della prestazione o consulenza.

I documenti e i supporti elettronici portati in visione dal paziente devono essere conservati rispettando le regole del rispetto del segreto professionale e, al momento della dimissione o alla conclusione della visita, riconsegnati al paziente.

1.11. - Ritiro referti

Qualsiasi documento relativo ad attività sanitarie (quali referti di esami di laboratorio o di esami strumentali, referti di Pronto Soccorso e di visite ambulatoriali, lettere di dimissione) deve essere consegnato in busta chiusa direttamente all'Interessato.

Il ritiro della documentazione sanitaria è ammesso anche da parte di persona diversa dall'interessato purché munita di delega scritta e con consegna in busta chiusa.

Per gli accertamenti HIV non è consentito il ritiro mediante delega.

1.12. - Attestazione di presenza in ospedale

Le dichiarazioni attestanti la visita, l'esame o il ricovero effettuati (es. giustificativo per il datore di lavoro) devono essere formulate in maniera tale che dalle stesse non possano derivare, per gli estranei, informazioni riguardanti lo stato di salute della persona interessata. L'attestazione deve essere generica e non deve riportare indicazioni sulla struttura di erogazione, né il timbro con la specializzazione del sanitario o ogni altra informazione da cui si possa evincere la patologia trattata.

2. DOCUMENTAZIONE CARTACEA E SANITARIA

2.1. - Tenuta e custodia

I documenti contenenti dati personali o dati relativi alla salute del Paziente, devono essere custoditi dai "Designati" e dagli "Autorizzati" al trattamento in modo da non essere accessibili a persone prive di autorizzazione (es. locali non accessibili al pubblico, armadi o cassetti chiusi a chiave).

I documenti contenenti dati personali o dati relativi alla salute del Paziente non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

In caso di locali aperti al pubblico, le cartelle e i fascicoli devono essere tenuti sulla propria scrivania facendo sì che i dati non siano visibili a persone non autorizzate.

In caso di assenza o allontanamento, anche temporaneo, dalla postazione di lavoro, è vietato lasciare incustoditi fascicoli, cartelle o documenti cartacei contenenti dati relativi alla salute del Paziente. In tal caso occorre chiudere la propria stanza, qualora rimanga incustodita senza personale all'interno, oppure riporre la documentazione in un armadio o cassetto chiuso a chiave.

2.2. - Comunicazione e trasmissione

I documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a colleghi che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se tali professionisti o operatori sono a loro volta "Autorizzati" al trattamento).

I documenti contenenti dati personali devono essere consegnati ai destinatari utilizzando buste chiuse o raccoglitori sigillati a garanzia dell'integrità - oppure effettuando la consegna personalmente - in modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto.

La trasmissione di documentazione sanitaria al domicilio del paziente - su richiesta dello stesso - deve avvenire in busta chiusa ed evitando di riportare sulla busta esterna riferimenti a specifici servizi/strutture dell'Azienda che possano rivelare lo stato di salute dell'interessato o il tipo di patologia.

Nel trasporto della documentazione tra un ufficio e l'altro, occorre adottare precauzioni per evitare la visibilità dei dati personali da parte di estranei (ad es. carpette o faldoni anonimi).

In caso di dati riservati o relativi alla salute occorre accertarsi che il tipo di spedizione sia idoneo a garantire l'integrità della documentazione e la ricezione certa da parte del destinatario.

E' proibito trasportare all'esterno del posto di lavoro qualsiasi documentazione contenente dati personali comuni e appartenenti a categorie particolari, salvo motivate esigenze di servizio e fermi restando gli obblighi di custodia.

2.3. - Archiviazione e distruzione

I documenti cartacei contenenti dati sensibili e/o giudiziari devono essere utilizzati dai "Designati" e dagli "Autorizzati" al trattamento solo per il tempo necessario allo svolgimento dei relativi compiti istituzionali e poi riposti in archivi o locali ad accesso controllato o, nei casi previsti, affidati al servizio di archiviazione.

Qualora sia necessario disfarsi di documenti cartacei contenenti dati personali, questi devono essere distrutti utilizzando gli appositi distruggidocumenti o, in loro assenza, strappandoli manualmente in modo da non essere più ricomponibili o leggibili.

3. UTILIZZO DI STRUMENTI INFORMATICI

3.1. – *User*-id e password

• L'accesso alle risorse informatiche dell'Azienda (PC, applicativi, banche dati, posta elettronica, ecc.) è consentito ai "Designati" e agli "Autorizzati" al trattamento dotati di credenziali di autenticazione formate da un codice di accesso (*user-id* o *username*) e da una parola chiave riservata (password) conosciuta solamente dal medesimo.

• Solamente i professionisti "Designati" al trattamento autorizzano - mediante apertura *ticket* con *mail* ad all'*Help Desk* del Servizio Informatico - il rilascio delle credenziali utente in favore del personale assegnato alle strutture rispettivamente dirette; ciò laddove il Servizio Informatico è Amministratore di Sistema. Nella richiesta di rilascio credenziali devono essere riportati obbligatoriamente i recapiti di telefono aziendale fisso e di telefono personale, generalità, Codice Fiscale, reparto/servizio di appartenenza dell'utente assegnatario della nuova *user-id*, riconducibile ad una singola persona. L'*help desk* provvederà all'abilitazione creando una *password* temporanea da modificare alla prima connessione.

• La *password* scelta dall'utente deve essere complessa, composta da almeno 8 caratteri alfanumerici, caratteri speciali (,.!?-=;:), lettere maiuscole, lettere minuscole e numeri.

• La *password* deve essere cambiata periodicamente almeno ogni sei mesi o secondo le specifiche scadenze appositamente comunicate. Va inoltre cambiata in ogni caso di sospetto utilizzo o conoscenza da parte di terzi.

• La password deve essere conservata con la massima attenzione e segretezza e non deve essere collocata a vista o in prossimità sulle postazioni di lavoro, non deve essere comunicata a terzi o lasciata in luoghi accessibili a terzi.

• *User-id* e *password* sono personali e non devono mai essere condivise tra più utenti anche se autorizzati al trattamento.

• Solo per motivate esigenze di servizio (ad es. in caso di assenza dal servizio) le credenziali possono essere rese note al responsabile della Struttura di appartenenza.

3.2. - Posta elettronica

• Ogni utente deve utilizzare la posta elettronica messa a disposizione dall'Azienda esclusivamente per necessità di lavoro e lo scambio di corrispondenza tra l'interessato e i propri familiari, amici e conoscenti deve essere assolutamente limitato nel tempo e nella quantità.

• La casella di posta elettronica è assegnata in maniera nominale ed univoca ad una persona fisica, pertanto ogni utente è direttamente responsabile sia da un punto di vista disciplinare che giuridico del suo utilizzo e del contenuto dei messaggi inviati.

• Nell'invio di una *e-mail* occorre prestare massima attenzione alla corretta digitazione dell'indirizzo del destinatario, specie in caso di comunicazioni riservate o relative alla salute.

• L'indirizzo di posta elettronica aziendale non deve essere utilizzato per l'iscrizione a servizi (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale etc.) non strettamente correlati alla propria attività istituzionale.

• L'utente non deve aprire o rispondere a comunicazioni *e-mail* inattese e/o di provenienza incerta o sospetta (anche se sembrano provenire da un mittente affidabile), contrassegnate come indesiderate (spam), contenenti allegati o *link* di cui non si conosce la natura e l'origine (estensione *.com .exe .vbs .scr .pif* ecc.), che possono

contenere *file* o programmi dannosi capaci di diffondere virus o programmi malevoli nell'infrastruttura aziendale o costituire attività di "phishing" mirate al furto di dati personali.

• E' vietato – ad eccezione di motivate esigenze di servizio - l'accesso alla casella di posta elettronica aziendale da computer pubblici in quanto alcuni dati potrebbero essere temporaneamente memorizzati nel disco locale e recuperati da un altro utente, se non cancellati in modo corretto.

• E', altresì, vietato l'accesso alla casella di posta elettronica aziendale mediante *wifi*-pubblici (ad es. aeroporti, hotel, ristoranti, ecc.) o altre reti non protette che espongono a rischi per la sicurezza dei dati.

• Ogni utente deve periodicamente cancellare o archiviare la posta elettronica in modo da evitare il riempimento della quota disco assegnata.

• Ogni utente deve predisporre, nell'ambito dell'apposita area "Preferenze" -> "Firme" della *webmail*, la firma in fondo ai messaggi avendo cura di dettagliare identità, reparto/servizio di appartenenza, numeri di telefono di contatti.

3.3. - *Personal computer*

• Il PC in dotazione deve essere utilizzato esclusivamente per ragioni di lavoro e per conto dell'Azienda.

• E' vietato connettere alla rete dati aziendale personal *computer* personali.

• In caso di necessità i dipendenti possono utilizzare un PC aziendale diverso da quello in dotazione, entrando in rete con la propria *username* e *password* di dominio AOMN.

• Durante la sessione di lavoro è necessario evitare che persone estranee e non autorizzate possano visualizzare la schermata del PC posizionando, se del caso, lo schermo in modo da limitarne la visibilità.

• Durante una sessione di lavoro non si deve lasciare il PC incustodito o accessibile da soggetti estranei: in caso di allontanamento - anche temporaneo - dalla postazione di lavoro occorre bloccare la postazione o disconnettere la sessione di lavoro.

• I programmi devono essere chiusi secondo appropriate misure di sicurezza per evitare la perdita dei dati.

• Il PC deve essere spento al termine della sessione lavorativa o in caso di assenza prolungata dalla postazione di lavoro, salvo diversa indicazione per necessità di accesso in *Smartworking.*

• Gli unici addetti autorizzati ad installare *software*, apportare modifiche alle impostazioni di sicurezza o di configurazione del PC (es. antivirus) sono i tecnici di *Help Desk* del Servizio Informatico. Nessun utente è autorizzato ad installare *software* o *hardware* diversi da quelli forniti dall'Azienda senza formale autorizzazione del Servizio Informatico.

L'uso di *software* contraffatto, ovvero con licenza d'uso contraffatta, costituisce un illecito penale e civile, secondo quanto previsto dalla normativa sul diritto d'autore.

• Ogni utente è tenuto a non interrompere le operazioni di aggiornamento pianificate del sistema operativo e degli antivirus, procedendo al salvataggio dei dati ed al riavvio del PC, qualora richiesto.

• I dati e i documenti elettronici contenenti dati sensibili devono essere archiviati sul *server* centrale dell'Azienda ed eliminati dall'*hard disk* del PC in dotazione.

• E' vietata la condivisione di documenti contenenti dati personali particolari su *cloud* (*dropbox, google drive, one drive, wetransfer.com*, ecc.) e server non aziendali.

3.4. - Dispositivi portatili e supporti di memoria

• I dispositivi portatili (*notebook*, *tablet*, ecc.) e i supporti di memoria rimovibili (ad es. CD, DVD, *pen drive*, memorie USB, ecc.) devono essere conservati in un luogo sicuro (stanze, armadi o cassetti chiusi a chiave) e mai lasciati incustoditi.

• E' vietato l'uso di dispositivi portatili e memorie al di fuori dall'Azienda, tranne che per motivate esigenze di servizio. L'utilizzatore è personalmente consapevole dei rischi per la protezione dei dati e delle conseguenti responsabilità in caso di perdita o violazione degli stessi.

• Salvo motivate esigenze, è tassativamente vietato trasferire, anche solo temporaneamente, copie di dati personali particolari (es. dati sanitari) su qualsiasi dispositivo portatile o memoria rimovibile.

• Nel caso in cui vi sia la motivata necessità di memorizzare dati relativi alla salute su dispositivi portatili o memorie rimovibili, l'archiviazione deve avvenire mediante impiego di idonei sistemi di crittografia e copie di backup.

• In sede di rimozione dei dispositivi di memoria occorre seguire le procedure di disconnessione sicura.

• E' obbligatorio assicurarsi che i dispositivi non vengano utilizzati da terzi e che non siano infettati da virus (procedere alla scansione del supporto).

• E' vietata - ad eccezione di motivate esigenze di servizio - la connessione dei dispositivi aziendali a *wifi*-pubblici (ad es. aeroporti, hotel, ristoranti, ecc.) o altre reti non protette, in quanto comportano rischi per la sicurezza dei dati.

• In caso di riutilizzo/dismissione dei dispositivi portatili e dei supporti di memoria, l'utente deve assicurarsi che si proceda, prima dello smaltimento, all'eliminazione permanente delle informazioni e dei dati memorizzati affinché questi non possano essere in alcun modo recuperati.

3.5. – Sistemi server e *Backup*

• E' obbligatorio utilizzare le cartelle *Home* utenti di rete e le cartelle di scambio di servizio/reparto per detenere dati aziendali necessari alle continuità di servizio.

• E' consigliato verificare almeno settimanalmente la presenza e consistenza dei dati contenuti nelle cartelle e comunicare tempestivamente eventuali errate cancellazioni dei medesimi. Il sistema informatico possiede una *data retention* per i dati utenti di 7 giorni. In caso di cancellazione di *file* con tempo superiore sarà impossibile recuperare i backup dei medesimi.

3.6. - Fotocopiatrici, stampanti e fax

• Occorre assicurarsi di non lasciare incustodite le stampe contenenti dati sensibili, specie se la stampante o la fotocopiatrice è condivisa con più utenti e si trova a distanza dalla postazione informatica. Le copie non necessarie devono essere rese illeggibili prima di essere eliminate.

• Fotocopiatrici, fax, stampanti di rete, devono essere sempre collocate in un luogo non accessibile a terzi non autorizzati.

• In caso di ricevimento via fax di documentazione contenente dati sensibili occorre provvedere all'immediato ritiro della stessa.

• Non si deve lasciare incustodita presso fotocopiatrici, fax, stampanti di rete documentazione contenente dati sensibili.

• Prima di inviare via fax documenti contenenti dati relativi alla salute occorre assicurarsi preventivamente che l'effettivo destinatario sia sul posto o comunque che il fax sia in un luogo protetto e presidiato, non accessibile a pubblico, e che non vi siano pertanto rischi di conoscenza da parte di soggetti estranei o non autorizzati.

• In fase di invio del fax occorre prestare la massima attenzione alla corretta digitazione del numero del destinatario.

• Sulla copertina del fax si consiglia di apporre la seguente formula: "Qualora il destinatario del presente fax non sia la persona indicata nella presente copertina, è pregato di dare immediata comunicazione al mittente, a mezzo telefono o per fax. Il destinatario della presente comunicazione deve distruggere immediatamente la documentazione ricevuta e in ogni caso potrà essere ritenuto responsabile dell'uso non autorizzato delle informazioni ivi contenute, erroneamente acquisite".