

Egr. Sig.

[*Titolo Cognome Nome del Designato*]

Direttore/Responsabile della Struttura

[*Descrizione Struttura*]

OGGETTO: Atto di nomina a Designato al Trattamento dei Dati Personali (art. 2-quaterdecies Codice privacy)

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 "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 - RGPD)";

Visto in particolare il disposto dell'art. 29 del RGPD inerente al trattamento sotto l'autorità del Titolare del Trattamento o del Responsabile del Trattamento;

Visto il D.lgs. 30 giugno 2003, n.196 recante il "Codice in materia di Protezione dei Dati Personali", così come da ultimo novellato dal D.lgs. 10 agosto 2018, n. 101;

Visto in particolare il disposto dell'art. 2-quaterdecies del D.Lgs. 196/2003 e la libertà organizzativa interna prevista dal RGPD;

Visto il Modello Organizzativo in materia di Protezione dei Dati Personali ("MOP") dell'Azienda Sanitaria Locale di Alessandria;

Visto in particolare l'art. 5.4 del MOP che prevede la nomina quali Designati al Trattamento dei Dati Personali da parte del Titolare del Trattamento dei Direttori delle Strutture Complesse e dei Responsabili delle Strutture Semplici a valenza Aziendale e delle Strutture Semplici a valenza Dipartimentale in cui si articola l'Azienda;

Con la presente, l'Azienda Sanitaria Locale di Alessandria, in qualità di Titolare del Trattamento (in seguito "Titolare"), Le comunica la nomina a Designato al Trattamento dei Dati Personali (in seguito "Designato"), ai sensi dell'art. 29 del Reg. UE 2016/679 (Regolamento Generale sulla Protezione dei Dati - RGPD) e dell'art. 2-quaterdecies del d.lgs. 196/2003 e s.m.i. (Codice della privacy).

Con la presente nomina Lei è pertanto autorizzato a trattare i dati personali relativi ai procedimenti ed alle attività inerenti all'Ufficio di appartenenza, anche per il tramite dei sistemi informativi impiegati dal Titolare ed a coordinare le attività di trattamento svolte dai soggetti autorizzati al trattamento appartenenti a detto Ufficio.

Si precisa che tutti i trattamenti dei dati personali, anche eventualmente quelli di cui all'articolo 9 ("Trattamento di categorie particolari di dati personali") e quelli di cui all'articolo 10 relativi a condanne penali e reati del Regolamento (UE) 2016/679, autorizzati al Designato dovranno essere

svolti esclusivamente nel rispetto delle istruzioni ricevute e di ogni ulteriore indicazione fornita dal Titolare del Trattamento.

I trattamenti che il Designato è autorizzato a svolgere sono quelli relativi all'ufficio in cui il Designato svolge la propria attività lavorativa e specificatamente elencati nel registro dei trattamenti approvato dall'Azienda e che il Designato dichiara di conoscere.

In ogni caso, con la presente nomina il Designato è autorizzato a compiere tutte le operazioni di trattamento, sia in forma cartacea che informatica, di dati personali contenuti all'interno di archivi e/o banche dati, il cui accesso e trattamento si rendano strettamente necessari per lo svolgimento delle attività, mansioni e ruolo funzionale svolto presso le strutture e i locali dell'Azienda.

Con la sottoscrizione della presente lettera di autorizzazione, il Designato dichiara di avere preso visione dell'informativa ai sensi dell'Articolo 13 del RGPD (reperibile sul sito istituzionale di ASL AL), nonché puntuali indicazioni in merito all'ambito del Trattamento dei Dati Personali consentito, le istruzioni operative e le procedure recanti le modalità di Trattamento dei Dati Personali (ai sensi dell'articolo 29 del RGPD), nello specifico:

- Compiti del Designato
- Istruzioni generali per il Trattamento dei dati;
- Istruzioni sull'uso degli strumenti informatici;
- Regole per una corretta tenuta delle Postazioni di Lavoro;
- Istruzioni sull'utilizzo della Posta Elettronica Ordinaria;
- Istruzioni sul Trattamento dei Dati in ambito sanitario;
- Modello Organizzativo in materia di Protezione dei Dati Personali ("MOP") dell'Azienda Sanitaria Locale di Alessandria (allegato).

Compiti del Designato

I compiti del Designato sono:

- a) verificare la legittimità dei trattamenti di dati personali effettuati dalla Struttura di riferimento;
- b) collaborare con l'Ufficio Privacy e con il DPO, al fine di consentire agli stessi l'esecuzione dei compiti e delle funzioni assegnate;
- c) accertarsi che il personale afferente alla Struttura Organizzativa di competenza, abbia sottoscritto la lettera di nomina ad Autorizzato al trattamento;
- d) individuare ed incaricare i Referenti per la Protezione Dati per la propria Struttura Organizzativa. I nominativi dovranno essere comunicati all'Ufficio Privacy;
- e) proporre il personale della propria articolazione organizzativa per le attività formative in materia di protezione dei dati;
- f) rapportarsi con l'Ufficio Privacy, al fine di adottare soluzioni di "privacy by design" e "privacy by default", ovvero di protezione dei dati fin dalla progettazione e per impostazione predefinita, prevedendo, già dall'origine e in considerazione del contesto complessivo ove il

trattamento si colloca e dei rischi stimati, un paradigma di trattamento e misure di protezione prefissate;

- g) procedere alla comunicazione delle modifiche intervenute ai trattamenti di competenza e verificare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria Struttura Organizzativa;
- h) individuare i Responsabili del trattamento ex art. 28 del GDPR e richiedere la loro nomina al Direttore Generale, mediante utilizzo del modello fornito dall'Ufficio Privacy e comunicare a quest'ultimo l'avvenuta nomina ai fini dell'aggiornamento del relativo registro;
- i) procedere alla comunicazione delle modifiche intervenute ai trattamenti di competenza e verificare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria Struttura Organizzativa;
- j) inoltrare tempestivamente all'Ufficio Privacy e al DPO le richieste pervenute, alla propria Struttura, da parte degli Interessati a questioni legate al trattamento dei dati;
- k) rilevare e comunicare tempestivamente all'Ufficio Privacy e al DPO i casi di violazione, anche potenziale, dei dati personali (Data Breach), verificatisi nell'ambito organizzativo di riferimento;
- l) verificare, con cadenza almeno semestrale, le abilitazioni rilasciate, per gli applicativi informatici, ai propri collaboratori e segnalare alla Struttura ICT eventuali cessazioni o modifiche nel rapporto di lavoro;
- m) inoltrare all'Ufficio Privacy, segnalando la necessità di redigere una valutazione di impatto per un determinato trattamento, le informazioni previste all'art. 35 GDPR sul trattamento in oggetto (descrizione del trattamento, finalità, valutazione delle necessità e proporzionalità del trattamento in relazione alle finalità, valutazione dei rischi e misure previste per affrontare i rischi), al fine di permettere all'Ufficio Privacy di dare avvio alla valutazione per la parte di propria competenza;
- n) verificare, una volta esaurita la finalità del trattamento, la corretta ed effettiva eliminazione dei dati raccolti.

Inoltre, il Designato ha il compito di coordinare i trattamenti dei dati personali nella Struttura/Ufficio di competenza, fornendo agli Autorizzati le istruzioni del caso, vigilando sull'osservanza delle disposizioni in materia.

Il Designato deve sempre attenersi alle norme del RGPD, al Codice della privacy (D.lgs. 196/2003 e s.m.i.), ai provvedimenti del Garante e alle istruzioni e misure di sicurezza comunicate dal Titolare, anche mediante Regolamenti interni.

Il Designato si impegna a frequentare i corsi di formazione e aggiornamento, organizzati dal Titolare, in materia di privacy e Protezione dei Dati Personali. Il Designato si impegna, altresì, affinché gli Autorizzati appartenenti alla sua Struttura partecipino ai corsi di formazione ed aggiornamento in materia.

Istruzioni generali sul trattamento dei dati

- 1) Il Designato è tenuto al rispetto ed all'applicazione dei principi generali in ambito di data protection indicati dall'art. 5 del Regolamento Europeo n. 2016/679 "principi applicabili

al trattamento di dati personali”, quali:

- ▶ i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell’Interessato (<<liceità, correttezza e trasparenza>>);
- ▶ i dati devono essere raccolti per finalità determinate, esplicite e legittime e, successivamente, trattati in un modo che non sia incompatibile con tali finalità (<<limitazione delle finalità>>);
- ▶ i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (<<minimizzazione dei dati>>);
- ▶ i dati devono essere esatti e, se necessario, aggiornati (<< esattezza>>);
- ▶ i dati devono essere conservati in una forma che consenta l’identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (<<limitazione della conservazione>>);
- ▶ i dati devono essere trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (<<integrità e riservatezza>>).

- 2) Il Designato deve rispettare le misure tecniche ed organizzative messe in atto dal Titolare.
- 3) Il Designato deve rispettare il Regolamento Aziendale per l’utilizzo delle postazioni di lavoro e le indicazioni della Struttura ICT relative all’utilizzo di posta elettronica e internet.
- 4) Il Designato deve rispettare il segreto d’ufficio e/o il segreto professionale. Il DESIGNATO sarà tenuto alla riservatezza anche dopo la cessazione del rapporto di lavoro o il trasferimento o eventuale revoca della nomina.
- 5) Il Designato deve curare che sia garantita, nella Struttura di competenza, la massima riservatezza, con specifico riferimento alle categorie particolari di dati (dati che rivelano l’origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale, 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).
- 6) Il Designato deve accertarsi che, all’interno della propria organizzazione, i soggetti Autorizzati al trattamento dei dati abbiano ricevuto apposita nomina.
- 7) Il Designato deve fornire agli Autorizzati le istruzioni per il corretto Trattamento dei Dati Personali ed eseguire successivamente gli opportuni controlli, vigilando sull’osservanza delle disposizioni impartite.
- 8) Il Designato deve informare prontamente il Titolare e il Referente Protezione Dati nominato dall’Azienda di ogni questione rilevante in materia.
- 9) Il Designato deve verificare annualmente con gli Amministratori di Sistema i livelli di abilitazione ai diversi gestionali/applicativi relativi ai singoli Autorizzati al trattamento e aggiornare periodicamente (almeno una volta l’anno) le relative autorizzazioni.

- 10) Il Designato deve procedere, se necessario, con l'individuazione di ulteriori misure di sicurezza da adottare, sia organizzative, sia fisiche, sia logiche e procedurali.
- 11) Il Designato vigila affinché siano evitate cessioni, consegne, copie, riproduzioni, comunicazioni e divulgazioni non autorizzate di dati personali da parte degli Autorizzati della propria Struttura.
- 12) Il Designato deve rispettare il divieto di fotografare utenti o colleghi nell'esercizio delle loro attività all'interno dell'Azienda.
- 13) Il Designato deve adottare le istruzioni sopra descritte in tutte le sedi, anche territorialmente dislocate, di competenza.

Istruzioni sull'uso degli strumenti informatici

L'accesso agli strumenti informatici (server, applicativi, posta elettronica) deve avvenire attraverso l'utilizzo del proprio profilo di autorizzazione, composto da username (codice identificativo personale) e password (chiave riservata) o altri strumenti di autenticazione messi a disposizione dal Titolare del Trattamento.

- 1) È necessario che le credenziali di accesso:
 - ▶ non siano condivise con altri soggetti;
 - ▶ siano custodite con accuratezza e non rese facilmente visibili/accessibili (es. retrostante tastiera del pc, post-it posto sulla scrivania/monitor, etc.);
 - ▶ non vengano memorizzate automaticamente dal sistema per un accesso più rapido;
 - ▶ non siano riportate in elenchi su file elettronici memorizzati sul desktop oppure conservati in agende poste sulla scrivania;
 - ▶ abbiano una password che rispetti i requisiti di sicurezza e complessità, così come definiti dal Gruppo Sicurezza di cui al Modello Organizzativo ICT.
- 2) I supporti removibili (pen drive, hard disk esterni, cd, dvd, etc.) che permettono di copiare/archiviare files e documenti esternamente al PC, sono da considerarsi strumenti di lavoro e come tali essere utilizzati dagli operatori cui la struttura abbia assegnato gli stessi.
- 3) Alcune regole per la gestione ed utilizzo dei supporti removibili:
 - ▶ cautela per evitare che il contenuto sia trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato;
 - ▶ divieto di uso in luoghi diversi da quelli della sede di lavoro e conservazione in luoghi sicuri (cassettiere o armadi chiusi a chiave);
 - ▶ l'operatore, se ritiene necessario portare con sé lo strumento, dovrà ritenersi responsabile in caso di furto o perdita dello stesso e farne tempestiva comunicazione al Titolare.
- 4) Se la struttura ha messo a disposizione degli operatori telefoni cellulari, questi ultimi dovranno rispettare le seguenti regole:

- ▶ non memorizzare immagini/video personali;
- ▶ non riportare numeri di telefono di propri familiari o conoscenti;
- ▶ usare smartphone criptati;
- ▶ attivare blocco schermo temporizzato con PIN o altro sistema per sblocco;
- ▶ non scaricare App per uso personale (social network, home banking, posta elettronica personale, acquisti);
- ▶ non effettuare backup automatici su Google, Whatsapp o sistemi simili;
- ▶ riversare su server dell'organizzazione video/immagini raccolti per fini lavorativi evitando di utilizzare Whatsapp, Dropbox o sistemi simili.

L'abuso o l'uso scorretto degli strumenti assegnati (computer, dispositivi portatili, posta elettronica, banche dati, collegamento ad Internet, credenziali di accesso, social network) costituiscono comportamenti contrari ai doveri di diligenza e fedeltà, punibili con sanzioni disciplinari e penali.

Regole per una corretta tenuta della postazione di lavoro

- 1) La postazione di lavoro è uno strumento da utilizzare secondo le regole della diligenza e della buona condotta e ciò rende ciascun operatore responsabile della sua corretta tenuta;
- 2) Ogni utilizzo non conforme può causare disservizi, costi di manutenzione, minacce di sicurezza, danni a persone o al patrimonio informativo del Titolare del Trattamento, da ciò ne deriva che ciascun utente è tenuto a rispettare la configurazione e gli strumenti applicativi messi a disposizione dall'organizzazione per lo svolgimento della propria mansione;
- 3) I documenti in lavorazione e le cartelle devono essere memorizzati in apposite aree di rete dedicate presenti sul server per evitare dispersioni o perdita di informazioni o accesso illecito agli stessi;
- 4) Non è permesso il salvataggio di file dell'organizzazione sulla memoria locale del PC, né in apposite cartelle locali, né sul desktop, per i quali non sono garantite operazioni di manutenzione, backup e ripristino dei dati, in casi di perdita;
- 5) Trattandosi di strumento di lavoro, non è consentito memorizzare sulla propria postazione documentazione personale (file, fotografie, video), installare dispositivi di comunicazione o memorizzazione (modem, masterizzatori) e scaricare software senza l'autorizzazione preventiva del Titolare del Trattamento o della Struttura ICT;
- 6) Al fine di evitare accessi illeciti a dati personali, l'utente è tenuto a:
 - ▶ adottare politiche dello "schermo pulito";
 - ▶ non lasciare incustodita la postazione con documentazione riservata visibile;
 - ▶ eseguire la procedura di logout dall'applicativo e/o dal sistema operativo tramite la funzione del blocca/disconnetti;
 - ▶ attivare screensaver il cui sblocco è reso possibile attraverso l'inserimento di password.

Istruzioni sull'utilizzo della posta elettronica ordinaria

- 1) La posta elettronica ordinaria, sia intestata all'Ufficio/Struttura, sia nominativa, è da considerarsi uno strumento di lavoro messo a disposizione dal Titolare del Trattamento.
- 2) Deve essere utilizzata solo per motivi strettamente connessi allo svolgimento dell'attività lavorativa.
- 3) Non deve essere considerata "privata" anche se recante il proprio nome e cognome.
- 4) Soggetti assegnatari di account di posta elettronica ordinaria sono responsabili del corretto utilizzo dello stesso e sono obbligati a rispettare anche i criteri definiti per l'accesso agli strumenti informatici.
- 5) È fatto divieto di utilizzare l'account messo a disposizione dal Titolare del Trattamento per:
 - ▶ trasmettere e ricevere documenti di natura personale;
 - ▶ fare re-inoltri dei messaggi su caselle di posta elettronica personale con dominio diverso da quello dell'organizzazione;
 - ▶ trasmettere documenti ufficiali dell'organizzazione recanti rilevanza giuridica verso terzi per cui è richiesto l'utilizzo della posta elettronica certificata istituzionale. Si rispettino, pertanto, le regole definite per una corretta gestione documentale informatica nelle more dei principi dettati dal Codice dell'Amministrazione Digitale (D.lgs. 82/2005 smi).
- 6) Per la trasmissione di documenti/dati/informazioni (es. bozze, documenti informali) contenenti categorie particolari di dati (es. dati idonei a rivelare lo stato di salute) è necessario utilizzare delle maggiori cautele, ovvero:
 - ▶ trasmettere i dati come allegato e non come testo nel corpo del messaggio;
 - ▶ cifrare i dati rendendo nota al destinatario la chiave crittografica tramite canali differenti da quelli utilizzati per la trasmissione stessa;
 - ▶ proteggere l'allegato con modalità idonee a impedire l'illecita o fortuita acquisizione dei dati trasmessi (es. password per l'apertura del file resa nota al destinatario tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati).
- 7) In ambito sanitario, la trasmissione di referti tramite posta elettronica è una pratica non corretta.
- 8) I messaggi di posta elettronica sono uno dei principali vettori di attacco ai sistemi informatici che rendono necessari accorgimenti particolari quali:
 - ▶ non aprire mail che risultano sospette;
 - ▶ diffidare da mail che, sebbene arrivate da indirizzi conosciuti, richiedono l'apertura di un allegato tramite l'inserimento di password o codici;
 - ▶ non procedere con l'avvio di codici eseguibili qualora la mail lo richieda.

Istruzioni sul trattamento di dati in ambito sanitario

Nel trattamento dei dati relativi alla salute delle persone, il Designato deve assicurare il rispetto, anche da parte degli Autorizzati al trattamento della propria Struttura, delle regole seguenti.

1) Dignità della persona

La prestazione medica e ogni operazione di Trattamento dei Dati Personali deve avvenire nel pieno rispetto della dignità dell'Interessato.

La tutela della dignità personale deve essere garantita nei confronti di tutti gli utenti dei servizi sanitari, con particolare riguardo ai soggetti più vulnerabili quali:

- ▶ disabili, fisici e psichici
- ▶ minori
- ▶ anziani
- ▶ pazienti sottoposti a trattamenti medici invasivi
- ▶ persone sieropositive
- ▶ donne che abbiano richiesto o effettuato l'interruzione volontaria della gravidanza
- ▶ persone offese da atti di violenza sessuale
- ▶ pazienti ricoverati nei reparti di rianimazione/terapia intensiva
- ▶ tossicodipendenti o persone affette da altre dipendenze (ad es. etilismo o ludopatia)

2) Trasparenza e informazione

In base alle norme vigenti (Reg. UE 2016/679, art. 9 par. 2 lett. h), non occorre il consenso dell'Interessato per finalità di diagnosi, terapia, cura ed assistenza sanitaria o sociale.

L'Autorizzato verifica che l'Interessato abbia ricevuto l'informativa sul trattamento dei dati relativi alla salute e che abbia firmato per presa visione il documento predisposto dal Titolare. Ove previsto, in luogo della firma per presa visione, l'Autorizzato può annotare di aver fornito l'informativa nel documento (cartaceo o digitale) predisposto dal Titolare.

E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

Laddove l'Interessato intenda esercitare un proprio diritto relativo al trattamento dei dati (es. richiesta di accesso o cancellazione di dati personali), l'Autorizzato trasmette la richiesta all'Ufficio Privacy (email: privacy@aslal.it) o al Responsabile della Protezione dei Dati Personali (email: dpo@aslal.it).

3) Riservatezza nei colloqui e nelle prestazioni sanitarie

L'Autorizzato deve tutelare la riservatezza dei dati personali e della documentazione in suo possesso riguardante le persone, anche se affidata a codici o sistemi informatici.

L'Autorizzato non deve diffondere, attraverso la stampa o altri mezzi di informazione, notizie che possano consentire l'identificazione del paziente.

L'Autorizzato presta particolare attenzione alle modalità di svolgimento dei colloqui con gli utenti dei servizi sanitari ed assistenziali (ad es. in occasione di prescrizioni o di certificazioni mediche), per evitare che le informazioni sulla salute dell'Interessato possano essere accidentalmente conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

È vietata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico.

L'Autorizzato cura che i documenti contenenti informazioni cliniche dell'Interessato non siano resi visibili a terzi non legittimati (es. cartelle infermieristiche poste in prossimità del letto di

degenza).

E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

4) Informazioni sullo stato di ricovero o sulla salute di un paziente

L'Autorizzato si attiene alle eventuali indicazioni del paziente (se cosciente e capace) circa i soggetti che possono essere informati del ricovero, del reparto di degenza o dello stato di salute.

L'Autorizzato rispetta l'eventuale richiesta dell'Interessato di non comunicare tali informazioni neanche ai terzi legittimati.

Le informazioni da fornire ai terzi legittimati riguardano la sola presenza nel reparto; L'Autorizzato si assicura dell'identità della persona prima di fornire ogni informazione.

L'Autorizzato non comunica informazioni sullo stato di salute, salvo che l'Interessato abbia manifestato il proprio consenso. In caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere del paziente, il consenso può essere manifestato da parte di un altro soggetto legittimato.

E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

5) Notizie su prestazioni di Pronto Soccorso

L'Autorizzato in servizio nel Pronto Soccorso, se ciò rientra nelle proprie mansioni, può dare notizia (o conferma), anche telefonica, dell'accesso di un paziente alla struttura ai soli soggetti legittimati: familiari, parenti o conviventi del paziente. L'Autorizzato si assicura dell'identità della persona prima di fornire ogni informazione.

L'Autorizzato di Pronto Soccorso si limita, in tal caso, a comunicare che è in atto o si è svolta una prestazione e non fornisce informazioni sullo stato di salute.

L'Interessato - se cosciente e capace - deve essere preventivamente informato (ad es. in fase di accettazione), e posto in condizione di indicare i soggetti che possono essere informati della prestazione di pronto soccorso. L'Autorizzato rispetta eventuali indicazioni specifiche o contrarie del paziente.

E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

6) Distanza di cortesia

L'Autorizzato verifica che siano rispettate le distanze di cortesia nelle operazioni di sportello, nell'acquisizione di informazioni sullo stato di salute e, in generale, nelle operazioni di trattamento di dati sanitari.

E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

7) Ordine di precedenza e di chiamata nelle sale di attesa (escluso Pronto Soccorso)

Al di fuori del reparto di Pronto Soccorso, nell'erogare prestazioni sanitarie, assistenziali o amministrative, che richiedono un periodo di attesa (ad es., analisi cliniche, visite ambulatoriali), l'Autorizzato rispetta le misure tecnico organizzative adottate dal Titolare per evitare la chiamata nominativa dei pazienti (ad es., uso di codici forniti all'utente in fase di prenotazione o accettazione).

Se la chiamata nominativa risulta necessaria (ad es. in funzione di particolari caratteristiche del paziente anche legate ad uno stato di disabilità), l'Autorizzato, ove possibile, cerca di instaurare un contatto diretto con il paziente per chiamarlo.

E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

8) Consegna di documentazione sanitaria

Per la consegna di documentazione sanitaria (es. certificati, referti, copie di cartelle cliniche) o di altra documentazione da cui si desuma lo stato di salute della persona (es. fatture, ricevute di prenotazione di prestazioni, etc.), l'Autorizzato si attiene alle istruzioni fornite dal Titolare e dal Direttore o Responsabile della Struttura (Designato).

In mancanza di diverse istruzioni, i documenti vengono consegnati solo in formato cartaceo ed in busta chiusa. Tali documenti vengono consegnati al diretto Interessato o a terzi soggetti legittimati (es. genitori del minore) o muniti di delega scritta accompagnata dal documento d'identità.

E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

9) Violazione dei Dati Personali

Il Designato informa immediatamente (e comunque entro 24 ore dal momento in cui ne è venuto a conoscenza) l'Ufficio Privacy (email: privacy@aslal.it) e il Responsabile della Protezione dei Dati Personali (email: dpo@aslal.it) di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

La presente nomina è da intendersi a tempo indeterminato e copre l'intera durata dell'incarico di Direttore/Responsabile della Struttura. Può essere revocata dal Titolare del Trattamento dei Dati Personali o può terminare in caso di interruzione del rapporto di lavoro, salvo eventuali e/o diversi accordi tra le Parti.

L'attività di trattamento individuata nel presente atto sarà soggetta a revisione almeno annuale; da ciò discende la possibilità che nel periodo intercorrente tra due revisioni le attività di trattamento possano differire da quelle ivi indicate. In tali casi il soggetto destinatario della presente si riterrà comunque autorizzato allo svolgimento dei trattamenti derivanti dalle attività conferite sulla base di specifica disposizione organizzativa sviluppata nelle forme individuate dal Titolare del Trattamento. Le casistiche nelle quali i trattamenti dovranno considerarsi autorizzati pur in assenza di specifica indicazione nel presente atto sono le seguenti:

- ▶ impiego temporaneo di personale in attività generalmente non di competenza del medesimo per la gestione di urgenze;
- ▶ impiego temporaneo di personale in attività generalmente non di competenza del medesimo per esigenze organizzative non superiori ad un mese;
- ▶ impiego di personale in attività caratterizzata da "turnazione" degli addetti la quale comporti lo svolgimento di attività non di competenza dell'unità organizzativa a cui è assegnato il soggetto.

Il Designato dichiara di aver ricevuto le istruzioni, di averne presa visione e di impegnarsi ad adottare tutte le misure necessarie alla loro attuazione.

ASL AL – SSA ICT
Ufficio Privacy

Preso visione della nomina a Soggetto Designato in data [gg/mm/aaaa] da parte del dott.
[Nome Cognome Designato]

Firma: _____